2015

Cyber Security - Business Plan

Fanshawe College

STAGE GATE 2

BUSINESS PLAN FOR NEW PROGRAMS

The Business Plan for new programs is developed using this template and in consultation with a Curriculum Consultant from the Centre for Academic Excellence (CAE). All sections of this template and all Appendices must be completed.

Completed Business Plans are submitted to CAE three weeks in advance of the next Senior Leadership Council (SLC) meeting. If endorsed at Stage Gate 2 by SLC, CAE will forward the required information to the Credential Validation Service, Board of Governors, and the Ontario Ministry of Training, College and Universities (MTCU).

1.0 Program Specifications

Proposed program title: Cyber Security
Proposed credential: ☐ Local Board Approved Certificate ☐ Ontario College Certificate ☐ Ontario College Diploma ☒ Ontario College Advanced Diploma ☐ Ontario College Graduate Certificate ☐ Collaborative Degree ☐ Degree
MTCU program code (if it exists): MTCU 63002 Information Security Technology
MTCU program code comparables: MTCU 73002 Information Systems Security
Proposed Classification of Instructional Program Codes, formatted as ##.####: 11.1003 – Computer and information systems security/information assurance *For additional information, please refer to most recent Classification of Instructional Programs (CIP) Canada published by Statistics Canada, available on http://www.statcan.gc.ca/.*
Projected four-digit National Occupational Classification Codes (3 maximum), formatted as ####: 1. 2171 Information systems analysts and consultants 2. 3.

For additional information, please refer to most recent National Occupational Classification (NOC) Canada published by Statistics Canada, available on http://www.statcan.gc.ca/.
Identify all deliveries of this or a comparable program that have been or are currently offered at Fanshawe (including CE and/or Regional Campuses): **Describe deliveries:** MTCU 63002 has not been delivered at Fanshawe College. MTCU 73002 is currently offered at Fanshawe College: Information Security Management (ISM1), Graduate Certificate, London Campus Network and Security Architecture (NSA1), Graduate Certificate, London Campus
Proposed program launch date: September 2017
Proposed intake(s): ☒ Fall ☒ Winter ☐ Spring ☐ Other:
Number of students in first intake: 36
Length of program: • Number of semesters: 6 semesters (plus three co-op placements) • Semester length in weeks: 15 weeks • Total program hours: 2031
Program delivery (check as many as apply) ☒ Web-facilitated (face-to-face) ☐ Blended ☐ Online ☐ Fast-track ☐ Accelerated ☐ Collaborative ☐ Weekend ☐ Other
Co-op program ☐ No ☒ Yes ☐ Experiential co-op (required to graduate) ☒ Mandatory co-op (not required to graduate but fee is mandatory) ☐ Optional co-op (not required and fee only charged if students opt in)

2.0 Executive Summary

Include the following information (600 words maximum):

a) Program overview, length, credential, description and suggested delivery options.
b) Explain how this program is aligned with the indicated program area of strength and/or growth. (150 words recommended maximum)
c) Local, regional, provincial and/or national fit/competition
d) Links to further educational opportunities
e) Student and labour market demand/support for the program; job opportunities for graduates
f) Resources required

a) This three-year Advanced Diploma in Cyber Security will provide students with the foundational Information Technology (IT) skills and knowledge necessary to be successful in the IT industry. Foundational technology topics will include network management/analysis, programming and scripting, operating systems, and database management. Building on those technology topics, the curriculum will also develop students' skills in the areas of risk analysis, cryptography, vulnerability testing, access control implementation, and security audit performance. Graduates of this program will be able to proactively implement sound security practices to mitigate security risks and respond quickly to security breaches and issues that may have occurred. They will also have the skills necessary to recommend IT security best-practices. They will also have been taught many of the foundational knowledge and skills required to seek industry-recognized certifications from CompTIA, ISACA, CISSP, and Certified Ethical Hacker after graduation.

Through lectures, hands-on laboratory activities, case study analyses, and research projects, students will enhance their technical abilities and develop their interpersonal, communication, organizational, and problem-solving skills. This program will also include three co-operative education work placements to further enhance and apply many of those skills.

This program will delivered face-to-face (web-facilitated).

b) This program aligns with "Information Technology", an institutional program strength and, more specifically, with "Information Security", a program area for growth.

c) Information technology or cyber security is a priority at the national level. The Government of Canada has supported and invested in numerous initiatives to safeguard networks and information and develop new tools and practices for digital security (e.g., Government of Canada: FedDev Ontario, 2011, Oct. 28; 2012, March 23; 2013, Sept. 6). In 2010, the Government of Canada launched its Cyber Security Strategy with $90 million over five years to implement the strategy and $18 million ongoing (Government of Canada: Public Safety Canada, 2012, Oct. 17). In 2012, the Government of Canada invested an additional $155 million over five years to further strengthen the federal information technology infrastructure (Government of Canada: Public Safety Canada, 2012, Oct. 17). With a growing number of highly publicized cyber-attacks, companies and institutions need to continuously invest in security products and practices that will protect their own and their clients' or customers' data and information. Already the cyber security market for industry and the public is between $80 and $150 billion (USD) per year (Information and Communications Technology Council, 2012).

d) Upon completion of this Advanced Diploma, students will be able to further their education with a series of Graduate Certificates specializing in specific areas of IT Security (Information Systems Management, Network Security Architecture), Public Safety, or Business. These Graduate certificates would provide students with higher level learning focusing on a specific program area in IT (e.g., security architecture, digital forensics, IT infrastructure management).

e) According to the Information and Communications Technology Council (2012), the increased threat of cyber-attacks or crimes has created a strong need for IT professionals that can design and operate critical systems infrastructure that can withstand those attacks. However, there is a shortage of skilled individuals who are able to fill those roles, and the ICTC suggests that industry and academia invest in developing that skilled labour force (ICTC, 2012). Graduates of this proposed program will have the knowledge and skills to fill such roles. Information Systems Analysts and Consultants (NOC 2171) includes occupations such as systems and informatics security analysts, planners, and consultants. That occupational group is projected to have increased numbers of new jobs in the London Census Metropolitan Aggregate (CMA), Ontario, and Canada: 22, 549, and 1,373 new jobs per year respectively.

f) It is forecasted that two new full-time faculty members will be required in the first year to teach in this three-year program. Additionally, one faculty member will be required to act as the Program Coordinator. Resources will also be required for curriculum development, lab equipment, software and faculty training. Additional capital expenses include renovations to existing classroom/lab space and the purchase and installation of equipment.

3.0 Academic Programming and Quality Assurance

3.1 Program Vocational Learning Outcomes
Consultation: CAE

→ See ***Appendix A: Form 1 – Program Vocational Learning Outcomes.***

3.2 Essential Employability Skills Learning Outcomes
Consultation: CAE

→ See ***Appendix A: Form 2 - Essential Employability Skills Outcomes.***

3.3 Program Description
Consultation: CAE and Registrar's Office

→ See ***Appendix B: Program Description.***

3.4 Course Descriptions
Consultation: CAE

→ See ***Appendix C: Program Curriculum.***

3.5 Relationship to Professional or Licensing Bodies
Consultation: CAE

→ See ***Appendix D: Regulatory Status Form.***

3.6 Curriculum Design and Delivery

See ***Appendix E: Curriculum Map - Program VLOs and EESOs.***

a) Provide rationale for curriculum design, including work integrated learning (if appropriate):
    1. Alignment with program vocational learning outcomes
    2. Alignment with essential employability skills outcomes
    3. Suitability for target populations(s)
b) Indicate where and how existing courses may be included in this new program.
c) Provide rationale for delivery methods (e.g., face-to-face, blended, online, fast track, accelerated, collaborative, weekend), including work integrated learning (if appropriate):
    1. Alignment with program vocational learning outcomes (industry expectations)
    2. Alignment with essential employability skills outcomes
    3. Suitability for target populations(s)

Consultation: CAE

a) In general, the program has been designed around six major cyber security topics or themes that continue throughout the program from introductory or foundational courses in the first semesters to highly specialized and applied courses in upper years:

- Public Safety
- Networking
- Programming and Scripting
- Databases
- Operating Systems
- Communication (Reasoning & Writing, Communication, Technical Writing and Presentation)

Since this program will be of interest primarily to direct-entry students, the first level of the program will provide students with the foundational Information Technology (IT) skills and knowledge necessary to be successful in the IT industry. Foundational topics will include network management/analysis, programming and scripting, operating systems, and database management. These foundational topics are also covered in the first semester of the Computer Systems Technician/Technology Diploma/Advanced Diploma and the Computer Programmer Analyst Advanced Diploma programs. Thus, students will be able to enter into any of those existing programs or this new program and transfer among them following the first semester. Direct-entry students may not have had much exposure to all areas of IT in high school, so this broad foundational curriculum and transfer pathways will allow these students to identify the area they are most interested in.

Building on the foundational topics, the upper levels of the program will develop students' skills in the areas of risk analysis, cryptography, vulnerability testing, access control implementation, and security audit performance. Students will learn how to proactively implement sound security practices to mitigate security risks and respond quickly to security breaches and issues that may have occurred. They will also acquire some of the foundational knowledge and skills required to write the certification exams for industry-recognized certifications from CompTIA, ISACA, CISSP, and Certified Ethical Hacker. The co-op placements will occur after levels 3, 4, and 5. It is expected that students' first co-op placements will likely be in a general IT role to allow them to apply the foundational knowledge and skills from the first three levels of the program. The students' second placements should allow them to

work in a security-themed role, likely interacting with end-users to deploy and manage security tools. The third co-op placement should focus on IT security and allow students to work with the monitoring tools or other non-invasive security tools or contribute to a security-themed project in the workplace or business.

In addition to the extensive amount of experiential learning opportunities throughout the curriculum, students will also develop their project management and research skills two of the courses in the last year of the program: "Managing & Budgeting Technical Projects" and "Research Project & Entrepreneurship". These courses have been included in the curriculum to support students as they learn to apply their technical skills in a workplace environment.

An external stakeholder panel meeting was held on October 6th, 2015. Panel members included representatives from IT companies such as Tech Alliance, Pyramid Cyber Security and Forensics, BlackBerry, eSentire, London Hydro, Info Tech, and Digital Extremes. All panel members were enthusiastic about the development of this program and strongly supported the vocational learning outcomes (See Appendix A and Appendix E) and several of the elements of this curriculum, formally recommending the following:

- Include a broad base of foundational knowledge and skills across multiple areas (i.e. networking, systems administration, programming, application development) to develop the "language of security" and expose students to technologies, tools, applications, and strategies in multiple areas. *(Level 1 programming; 6 themes that build throughout the program; progression of co-op placements)*
- Provide opportunities for students to develop their creative thinking and communication skills for solving security issues and convincing clients/stakeholders of the need for security tools. *(Communication theme)*
- Incorporate numerous opportunities for hands-on, experiential learning to allow them to reinforce their knowledge of the "language of security" and build their confidence with using tools. *(Laboratory activities, case study analyses, research projects; progression of co-op placements)*
- Consider providing students with the opportunity to conduct research or innovate that contributes to the College and/or the open source community. *(Research project)*

b) The following existing courses, primarily at the introductory level, are being incorporated into this new program:

- INFO-1135 Networking Fundamentals
- INFO-1150 Programming Fundamentals
- INFO-1120 Database Fundamentals
- INFO-1178 Configuring Windows Client
- INFO-1124 Computer Security Concepts
- INFO-5096 Managing & Budgeting Technical Projects
- WRIT-1043 Reasoning & Writing for IT/WRIT-1034 Reasoning & Writing – EAP
- COMM-3047 Communication for IT Professionals
- COOP-1020 Co-operative Education Employment Prep.
- CRIM-3001 Criminology (General Education Elective – Mandatory for this program)

While there is some overlap with curriculum topics in the existing Diploma and Advanced Diploma programs in the School of IT that course developers will be able to draw on (e.g., networking,

programming, operating systems), the curriculum in this program emphasizes the security-related knowledge and skills for each of those topics (e.g., securing a network, evaluating code to find and fix security issues, identifying common security threats for different operating systems).

There is also synergy with curriculum topics in the existing security-themed Graduate Certificates (e.g., network security architecture) although learning outcomes and evaluation strategies will be adapted for the Advanced Diploma credential. Students in this Advanced Diploma program will be exposed to a wide range of IT security issues, tools, and techniques while students in the Graduate Certificates specialize in a particular area (e.g., information systems management, network security architecture).

c) This program will be delivered face-to-face (web-facilitated) and include three co-operative education placements to provide further opportunities for experiential learning. This program will be of interest primarily to direct-entry students, so they will benefit greatly from the face-to-face interactions with instructors and peers and from the opportunity to gain real work experience. In-class and on-the-job supervision and support will also help students to develop or enhance their communication and interpersonal skills (essential employability skills). As discussed in part a) above, an external stakeholder panel of IT industry professionals strongly supported the inclusion of as much hands-on or experiential learning in the program as possible.

3.7 Research and Innovation

a) Describe how research and innovation will be included in the program (Policy 2-B-02).
Consultation: Centre for Research and Innovation

Throughout the entire program, students will complete simulations, case studies, and hands-on laboratory activities that will develop their research skills and allow them to identify or develop innovative solutions to security issues or problems. The nature of the IT security industry requires subject matter experts to be continual learners, in defense of newly emerging cyber security threats.

An external stakeholder panel meeting was held on October 6th, 2015 with IT industry professionals from companies such as Tech Alliance, Pyramid Cyber Security and Forensics, BlackBerry, eSentire, London Hydro, Info Tech, and Digital Extremes. All of the panel members supported the inclusion of research and innovation activities throughout the program. In particular, they recommended providing students with the opportunity to conduct research or innovate in ways that will contribute to the College or the IT/open-source community. They also recommended that students have the opportunity to develop and deliver security awareness programs. Thus, the “Research Project” course in the last semester of the program will be designed to allow students to focus on a security topic or issue of interest to them or for a simulation or live client, depending on community partnerships. Fanshawe is in an ideal location to take advantage of the variety of industry technology partners that London has to offer. In the Research Project course, students will evaluate an IT security topic or case, research possible technologies or techniques for addressing the issues within the case, develop a solution, and present their research and findings to their peers or to a live client.

Based on the recommendations from the external stakeholder panel meeting, the School of IT will continue to reach out to industry partners to find organizations that are looking for assistance with the design of security solutions (i.e. tools, scripts) that the students can design, develop, and present to those organizations.

In the summer of 2015, the School of IT discussed potential new internationalization initiatives with the Hague University in the Netherlands. The School of IT currently has an exchange agreement with this University, but they are interested in looking into research opportunities in a security-related field. In the future, the School will be able to explore the potential for students to conduct research abroad or in conjunction with students in the IT security-related programs at the Hague University.

In the winter of 2016, Fanshawe College will be hosting a student on campus who will be completing a research internship under the supervision of a faculty member in the field of governance, audit, risk management and compliance. In the future, there will be opportunities for students to collaborate on research with this institution and others.

4.0 Fit of Program

4.1 Gap Analysis

a) How is the program similar to or different from existing programs at the College?

b) What impact will this program have on existing programs at the College? Does the proposed program provide additional breadth to our program offerings, or does it add specific disciplinary depth (i.e., would this program be part of a cluster of like programs)?

c) Are there similar programs being offered at colleges, universities or private institutions provincially, nationally and/or internationally? If yes, provide profile of key competitors including location and a brief description and how they differentiate themselves.

d) How else is the industry need being met if not provided in the options listed in c) above (e.g. regulatory body or in-service training)?

e) What makes this program unique from similar existing programs?

If the existing/proposed program is similar to others, consideration will be given to whether the program has differentiating features. For example, whether the existing/proposed program proposes innovative delivery methods, focuses on teaching and learning or specific student population(s), and builds on niche areas of program and/or research strength (Ministry Policy Guide for Applying for Ministerial Consent; 2014, p. 3).

Consultation: CAE, Strategy & Planning, External Resources

a) and b) As described in Section 3.6, this program will add breadth and depth to the program options available to students. This program will expose students to a wide range of topics that cut across many of the existing programs (e.g., network management/analysis, programming and scripting, operating systems, database management), but this program will emphasize the security knowledge and skills that can be applied in each of those areas (e.g., risk analysis, cryptography, vulnerability testing, access control implementation, security audit performance).

c) This program will be classified under the same MTCU code as the Computer Security and Investigations program at Fleming College and the Technologie de L'Information – Securite Informatique at La Cité Collégiale. Seneca College and Sheridan College offer similar programming as degrees.

Program	Institution	Differentiating Features
Computer Security and Investigations, Advanced Diploma (MTCU 63002)	Fleming College	• Acquire knowledge and skills required for industry certification exams: o CCNA – Cisco Certified Network Architect o CCE – Certified Computer Examiner o Security+ o Network+ o A+ o Linux+ o MCSE – Microsoft Certified System Engineer o CISSP- Certified Information Systems Security Professional (student level qualification) o CEH – Certified Ethical Hacker o EnCE – Encase Certified Examiner • One "Applied Project" in Level 6 that is a team-based project for an enterprise sponsor or a co-op placement • Course topics include law, justice, and criminology; emphasis of the program appears to be on policing and IT security • Pathway: UOIT Bachelor of Information Technology in Networking and IT Security
Technologie de L'Information – Sécurité Informatique, Advanced Diploma (MTCU 63002)	La Cité Collégiale	• Technical terminology used in the program is bilingual • Institute of Technology also offers Cisco Networking Academy courses • Leads to CCNA certification and part of the routing and communication CCNP certification • Course topics focus on IT fundamentals (e.g., networking, programming) with additional courses in ethics, project management, security planning and management, and cryptography • Pathway: Transfer from Computer Systems Engineering or obtain specialization following a degree
Bachelor of Applied Technology (Informatics and Security), Degree (MTCU 80521)	Seneca College	• Co-op program • Emphasis on informatics, security, and law with practical applications

		• Professional options in the last three semesters (specialize in areas of interest)
Bachelor of Applied Information Sciences (Information Systems Security) (MTCU 80509)	Sheridan College	• Internship up to 28 weeks in length • Topics include computer security, Information Systems (IS) intrusion detection and prevention, ethical hacking, database security, malicious code – design and defense, security auditing

d) The industry need has traditionally been met by in-house training and professional development. Security is a relatively new theme emerging in the IT industry and many currently employed professionals have had no formal training in this area. Many are self-taught through reading security articles and dealing with specific security incidences within their organization. Others have taken courses and gained industry certifications through private training facilities in order to learn about security practices. There are many certifications that these professionals may look at depending on their positions and specific job duties. These training programs are often vendor-specific as they are delivered by a company or organization with ties to a company that manufactures security products, such as CISCO or VMware, and often focus on only one area of expertise, such as governance or penetration testing.

Although industry training in this field has typically occurred on-the-job, the information and Communications Technology Council (2012) suggested that industry and academia invest in developing programming that will improve the skill level of the labour force (See Section 5.2 for more information about labour market trends).

e) There are several differentiating features of this program as it will be offered here at Fanshawe College:

- This program builds on existing strengths and expertise in the School of IT and aligns with an institutional program strength and an area for growth as outlined in the College's Strategic Mandate Agreement (SMA).
- This program is a collaboration with the School of Public Safety and leverages the collective expertise of both school faculties.
- This program includes three co-operative education placements that provide students with real-world work experience that will enhance their learning and help them build their resumes and connect with potential employers.
- The program will provide students with much of the foundational knowledge and skills required to write the certification exams for industry-recognized certifications from CompTIA, ISACA, Certified Information Systems Security Professional (CISSP), and Certified Ethical Hacker (CEH).
- Fanshawe College is in an ideal location to take advantage of the variety of industry technology partners that the London region has to offer.
- There are six major topics or themes that are woven throughout the program to provide students with a broad base of foundational knowledge and skills across multiple areas and exposure to technologies, tools, applications, and strategies in multiple areas: networking programming and scripting, databases, operating systems, public safety, and communications.

- There are numerous opportunities for research and innovation throughout the program and culminating in the "Research Project & Entrepreneurship" course in the last semester of the program (See Section 3.7).
- Students will have the opportunity to use innovative tools and technologies from the industry: biometric devices, firewalls and other intrusion prevention systems, and open-source tools for scripting, network design, and penetration testing.
- There is the potential for numerous pathways options including transfer among Diploma/Advanced Diploma programs in the first semester; further specialization with Graduate Certificates in the Schools of IT, Public Safety (in development), and Business; and dual credit options/Special High Skills Major programs for high school students (See Section 4.4)

4.2 Key Performance Indicators (KPIs)

Please complete this table with the three most recent years of published data* for similar programs at your college only (minimum one, maximum three). Similar programs may include programs at the same or different credential levels, and transfer opportunities. Please add additional rows as needed.

Program		Academic Year Of Graduation	2011-2012	2012-2013	2013-2014
MTCU Title	MTCU Code				
Computer Systems Technology	60505	Graduate Count	41	36	69
		Employment Rate**	94	88	91
		Employment Rate in a Related Field***	85	81	72
Computer Programmer Analyst	60503	Graduate Count	37	28	57
		Employment Rate**	73	95	87
		Employment Rate in a Related Field***	73	86	79
Information Systems Security	73002	Graduate Count	24	14	68
		Employment Rate**	67	71	56
		Employment Rate in a Related Field***	17	43	25

*KPIs are to be calculated in accordance with the methods prescribed by MTCU. KPIs are based on graduates of MTCU approved full-time postsecondary programs whose funding status is shown in the graduate record layout as MTCU operating grant, Co-op Diploma Apprenticeship or Second Career, and who were surveyed by telephone.

** Employment Rate = (number of survey respondents employed Full-time or part-time, related or unrelated) / (number of survey respondents in labour force)

*** Employment Rate in a Related Field = (number of survey respondents employed Full-time or part-time, related) / (number of survey respondents in labour force)

Additional explanation/information that contextualizes the KPI outcomes above, such as student demand or labour market analysis, may be provided. (400 words recommended maximum)

As shown in the table above, employment rates have been high for the School of Information Technology's existing Advanced Diploma programs for the last three years. At least 88% of graduates from the Computers Systems Technology program and at least 73% of the graduates from the Computer Programmer Analyst program have obtained employment with at least 72% and 73%, respectively, finding employment in a related field. This demonstrates that Fanshawe College's School of IT is effectively preparing graduates for the workplace and that there is demand for skilled professionals in the IT industry. This new Cyber Security Advanced Diploma will complement these existing offerings and prepare graduates specifically for the security sector within the IT industry.

Also shown in the table above is the employment rate information for the Information Systems Management Graduate Certificate. These rates reflect the fact that most of the students in that program are international students many of whom complete the program in combination with another Graduate Certificate to improve their chances of eligibility for a three-year work visa. Those graduates are sometimes looking for employment in other areas of IT rather than only for positions focusing on IT security. They may also begin employment in another area of IT or another field in order to gain Canadian work experience that may be required for employment directly in an IT security field.

Information Systems Analysts and Consultants (NOC 2171) includes occupations such as systems and informatics security analysts, planners, and consultants. That occupational group is projected to have increased numbers of new jobs in the London Census Metropolitan Aggregate (CMA), Ontario, and Canada: 11%, 5%, and 6% respectively. Those percentages equate to 176 new jobs between 2014 and 2021 or 22 new jobs/year in the London CMA; 4,389 new jobs or 549 new jobs/year in Ontario; and 10,984 new jobs or 1373 new jobs/year across Canada. (See Appendix J for further information about the labour market projections for this occupational group).

According to the Information and Communications Technology Council (2012), the increased threat of cyber-attacks or crimes has created a strong need for IT professionals that can design and operate critical systems infrastructure that can withstand those attacks. Already "projects related to collaboration, security, and cloud computing are among the most common contributors to labour force expansion in Canada" with three emerging occupations: Communications Infrastructure Engineers (CIE), IT Security Specialists, and Ethical Hackers (ICTC, 2012). However, there is a shortage of skilled individuals who are able to fill those roles, and the ICTC suggests that industry and academia invest in developing that skilled labour force (ICTC, 2012). Graduates of this proposed program will have the knowledge and skills to fill such roles.

How many other colleges within <u>your region</u> are approved for funding to offer programs in this same MTCU code?

There are two other colleges that are currently approved for funding to offer programs in this same MTCU code: Fleming College and La Cité Collégiale (Offered in French only).

*Please refer to the APS-MTCU Table available on the CAAT Extranet Site, in the Programs Section, for a complete list of programs approved for funding through the College Funding Framework, at http://caat.edu.gov.on.ca/ (user name: caatsite; password: 900Mowat).

4.3 Partnerships Supporting New Program

a) List any new internal or external partnerships that may develop if this program were to be delivered.

b) What, if any, alliances are possible to reduce costs, increase speed to market and increase market coverage?

c) How are the external stakeholders willing to support the proposed program? (check as many as apply)

☒ Continuing on Advisory Committee ☐ Teach a course

☒ Provide placement or experiential learning (e.g. co-op, field placement, mentorship)

☒ Present as a guest speaker ☒ Provide a tour

☒ Research (project, partnership etc.) ☐ Donation, Scholarship, Award

☐ Other:

On-going discussions between the School of IT and the School of Public Safety have identified several possible options for shared curriculum development (for this program and other programs being explored) and/or for providing pathways for students to transition between the two Schools. Given the overwhelming support from IT industry stakeholders, this Advanced Diploma is being developed to meet the specific needs of the IT industry while still exposing students to broader cyber security concerns in the field of Public Safety. Two additional programs under development, Digital Forensics and Business Intelligence will involve greater collaboration and shared curriculum among the IT, Public Safety, and Business Schools.

Over the last year, the University of Gloucestershire, The University of South Wales, Southhampton University, Royal Halloway University of London (UK) the Hague University (Netherlands), and Davenport University (US) have expressed interest in collaborating with the School of IT at Fanshawe College for research projects. Further discussions will occur to confirm those opportunities and explore the potential for academic exchanges and degree completion pathways.

Darlene O'Neill, Senior Manager of Employment and Student Entrepreneurial Services, has indicated that the employment rate in this area is high, and she is confident that in partnership with the Co-operative Education Consultant, the students will be successful in achieving work terms.

4.4 Pathways to and from Proposed Program and Programs

a) Drawing on the gap analysis, are any program pathways anticipated or under negotiation to and/or from this program (internal and external)? If yes, describe how the existing/proposed program supports student mobility.

The Ministry will consider whether the program offers students options for transfer from other programs/institutions and to other programs/institutions. In addition, the Ministry will consider the applicant's credit transfer agreements, if applicable, and inter-institutional collaboration more generally. (Ministry Policy Guide for Applying for Ministerial Consent; 2014, p. 6)

b) Describe any special features of this pathway (e.g., laddering, bridging).

c) How does this program fit into the provincial and national credit transfer framework? (ONCAT, PCCAT)?

Consultation: CAE

a) and b) The foundational courses in Level 1 of this program are also covered in the first semester of the Computer Systems Technician/Technology Diploma/Advanced Diploma and the Computer Programmer Analyst Advanced Diploma programs. Thus, students will be able to enter into any of those existing programs or this new program and transfer among them following the first semester as they identify the area they are most interested in.

The new program will provide students with a pathway into a variety of Graduate Certificates in IT, Public Safety, Business or other areas. Graduates who also complete one of the School of IT's security-themed Graduate Certificates can take advantage of the pathway into a Master's degree at University of Gloucestershire in the UK. Additional degree completion pathways will be explored both in Canada and abroad.

Opportunities for participation in the Specialist High Skills Major program with local area high schools are also being explored in connection with the existing programming in the School of IT. There is the potential for creating a dual credit within the Thames Valley District School Board.

c) This new program will fit into the provincial and national credit transfer frameworks.

4.5 How will this program help support the College's enrolment growth strategy?

This program aligns with "Information Technology", an institutional program strength and, more closely, with "Information Security", a program area for growth as outlined in the Strategic Mandate Agreement (SMA).

Additionally, this program aligns with Goals 1 and 3 from the College's Strategic Framework as described below:

- *Goal 1: Grow enrolment by 15% over 5 years to support local, regional, provincial and national requirements for skilled labour and post-secondary training*.
  This program will assist in growing enrollment by bringing in an estimated 36 new students by the Fall 2017 term and an additional 36 students for the Winter 2018 intake.
- *Goal 3: Provide a premier learning, student life and career preparation experience within the Ontario College system.*
  This program is designed to provide students with numerous experiential learning opportunities in the form of activities such as co-operative education placements, case studies, and practical laboratory exercises.

This program also aligns with strategies outlined in the Integrated Master Academic Priorities Plan (iMAPP) in that it is being developed to meet a specific and significant labour market need for skilled IT security specialists. This program will also address three of the pedagogical culture shifts reported in the iMAPP: research and innovation, entrepreneurship, and global outlook. Section 3.7 outlines the research and opportunities that will incorporated into this program. Basic entrepreneurship skills are

introduced in “Research Project & Entrepreneurship” in the final semester to prepare students to manage and promote their own IT security business or product development. The curriculum and case studies, simulations, and/or research projects with emphasize the global impact of cybercrimes and cyber security solutions.

5.0 Demand for Program

5.1 Student Demand

a) Provide evidence to validate student demand and/or societal need. (e.g. Student surveys, enrolment summaries and growth trends for similar programs, system enrolments and projected growth, or demographic projections for relevant sub populations)

b) Indicate which student populations are most likely to be attracted to the program:

Persona Groups

☒ Direct

☒ Non-direct

☒ International

☐ Other (identify):

c) Include an assessment of whether this program will draw students away from existing College programs or complement existing programs.

Consultation: Registrar’s Office, Recruitment, International, Strategy & Planning

a) Fleming College currently offers a similar program (MTCU 63002). That program is also offered in French at La Cité Collégiale. Application and enrolment data for the last four years are presented in Appendix I and show interest in this type of program. Over the last four years, application and enrolment numbers have been consistent with an average of 83 applicants per year for approximately 31 students enrolled in the program each year.

At Fanshawe College, there is growing expertise in the area of information security in both the School of Information Technology and the School of Public Safety.

The program was given verbal support from the International recruitment team at a meeting in September 2015. The international recruiters indicated that this program would be attractive to international students especially from India and Nigeria.

b) Direct-entry and International students will be the main student populations most likely to be attracted to this program.

c) It is possible that this program could draw a few students from the current programs in Computer Systems Technician/Technology and Computer Programmer Analyst programs, but because the subject matter is very different between the three programs, it is anticipated that this will be a low number. Even if a small number of students were to leave the existing Diploma/Advanced Diploma programs, their leaving would not put these programs into jeopardy due to their high enrollments now. As described in Section 3.6, this program and the existing programs listed here cover the same foundational material in their first semesters, so it is also possible that a few of the students who are

drawn to Fanshawe College for the new Cyber Security program will transfer into one of the existing programs. The three programs are complementary to each other with each program leading students into a different area of IT employment. This should result in a net zero enrollment change between the programs.

5.2 Labour Market Demand

a) Provide evidence to validate employment demand from some or all of the following:

1. Trend data (employment trends for related employment)
2. Feedback from and support of the Program Advisory Committee
3. Feedback from external stakeholders
4. Other data sources (e.g., London Economic Development Corporation)
5. Letters of employer support (attached as appendix)

1. Information Systems Analysts and Consultants (NOC 2171) includes occupations such as systems and informatics security analysts, planners, and consultants. That occupational group is projected to have increased numbers of new jobs in the London Census Metropolitan Aggregate (CMA), Ontario, and Canada: 11%, 5%, and 6% respectively. Those percentages equate to 176 new jobs between 2014 and 2021 or 22 new jobs/year in the London CMA; 4,389 new jobs or 549 new jobs/year in Ontario; and 10,984 new jobs or 1373 new jobs/year across Canada. (See Appendix J for further information about the labour market projections for this occupational group).

2. Industry representatives at the Information Security Management Program Advisory Committee (PAC) meeting from June 30th, 2015 indicated a growing industry need for security professionals. They suggested that in order to be successful in the security field, one has to be fluent in technology and have a mixture of theoretical knowledge and practical skills. The PAC members also emphasized a need for curriculum in the areas of mobile, privacy laws, programming, risk management, incident response and project management. This program will address all of these recommendations as well as the recommendation that students need to have a recognized industry certification along with their credentials. This will be accomplished by preparing them to explore a series of industry-recognized certifications.

3. An external stakeholder panel meeting was held on October 6th, 2015. Panel members included representatives from IT companies such as Tech Alliance, Pyramid Cyber Security and Forensics, BlackBerry, eSentire, London Hydro, Info Tech, and Digital Extremes. All panel members were enthusiastic about the development of this program and strongly supported the vocational learning outcomes (See Appendix A and Appendix E) several of the elements of this curriculum as described in Section 3.6. In addition to supporting the curriculum, the external panel members indicated that graduates of this program will be in high demand in this industry. They shared the following points about trends in the industry and how this program can help to address labour market needs:

- When asked about the importance of the credential that students receive and whether or not graduates of this program would be able to compete with graduates of Degree programs, the external stakeholders indicated that they look for students with Diploma and Advanced Diploma credentials because graduates of those programs have stronger technical skills.
- The external stakeholders all agreed that employers who are hiring security analysts are looking for security specialists who know a little about networking, operating systems, programming,

databases, etc. rather than network specialists, for example, who know a little bit about security.

- The panel members also agreed that practical experience in the form of laboratory activities, case studies, simulations, research projects, and work term placements is preferred by employers over industry certifications. Of course, if two candidates for a job have the same amount of experience, the candidate who has earned industry certifications would be preferred.
- The top three trends in the IT industry, as identified by the external stakeholder panel, include the growth of the "internet of things", the evolution of identity and device management options and requirements, and an awareness of network technology trends and their impacts on information security. All three trends will require IT professionals with a security specialization.

4. According to the Information and Communications Technology Council (2012), the increased threat of cyber-attacks or crimes has created a strong need for IT professionals that can design and operate critical systems infrastructure that can withstand those attacks. Already "projects related to collaboration, security, and cloud computing are among the most common contributors to labour force expansion in Canada" with three emerging occupations: Communications Infrastructure Engineers (CIE), IT Security Specialists, and Ethical Hackers (ICTC, 2012). However, there is a shortage of skilled individuals who are able to fill those roles, and the ICTC suggests that industry and academia invest in developing that skilled labour force (ICTC, 2012). Graduates of this proposed program will have the knowledge and skills to fill such roles.

5. Please see Appendix K for a letter of support from Darlene O'Neill, Senior Manager of Employment and Student Entrepreneurial Services. Darlene has indicated that the employment rate in this area is high, and she is confident that in partnership with the Co-operative Education Consultant, the students will be successful in achieving work terms.

6.0 Feasibility of Program

6.1 Multi-Year Enrolment Projections (headcount)

Consultation: Registrar's Office

	2017/18	2018/19	2019/20	2020/21	Ongoing
Year One	138	154	174	192	192
Year Two		122	134	154	168
Year Three			58	122	136
Year Four					
Number of Graduates	0	0	0	58	72
Total Enrolment	138	276	308	468	496

*** Values represent enrollment for a Fall and a Winter intake each year.**

Fall Intake	Fall	Winter	Spring
Year 1	Level 1	Level 2	Off
Year 2	Level 3	Co-op 1	Level 4
Year 3	Co-op 2	Level 5	Co-op 3
Year 4	Level 6		

Winter Intake	Fall	Winter	Spring
Year 1		Level 1	Level 2
Year 2	Level 3	Co-op 1	Level 4
Year 3	Co-op 2	Level 5	Co-op 3
Year 4	Level 6		

6.2 Human Resources

a) Include staffing plan for program, up to and including full implementation.

1. Estimate the staffing requirements that are above the existing HR complement.
2. Would there be any changes to current staffing arrangements in order to implement this new program?
3. Would there be any additional training needs?

Consultation: Human Resources, OD&L, other Schools

b) Student Services

1. What other Learner / Student Success Services are required?

Consultation: Student Success

a) Initially, at least two new full-time faculty members will be required to teach in this program or to replace faculty from another program within the School of Information Technology assigned to teach in this program. Given the level of specialization in this program, it will be difficult to deliver the program primarily with part-time faculty members.

Some of the current faculty members will need additional training to prepare them to teach the content required to prepare students for writing the industry exams upon graduation. Existing faculty may require funding to write industry-specific certifications to maintain currency in their fields of expertise.

This program will also require a faculty member to perform coordinator duties.

b) Students will be connected to Fanshawe College's student success, accessibility, and accommodations services through the Student Success Advisor in the School of IT and the International Office and the English Language Institute if required by international students.

Students will be assisted by the Co-operative Education Consultant in their search for co-op positions. Students will also be encouraged and supported in the development of their co-curricular record.

6.3 Ministry Funding

Consultation: CAE

See ***Appendix F: Program Delivery Information (PDI) Form to Calculate Program Funding Parameters.***

6.4 Tuition Fees

Consultation: Registrar's Office, Financial Planning, CAE

Approved Postsecondary (APS) Program MTCU Table

- **Wt** - Program Weight for funding purposes: __1.0__
- **FU -** Program Funding Units for funding purposes: ___3.8___
- Proposed annual tuition fee: $__2766.32__
- Fees: Regular Yes ☑ No _____

  High Demand Yes _____ No ☑
- What tuition and ancillary fees are being charged by other colleges for similar programs?

Program	Location	Tuition	Ancillary Fees
Computer Security and Investigations (MTCU 63002)	Fleming College	Domestic: $2851.04 per term International: $7140.00 per term (Fall 2015)	Domestic: $701.85 total International: $807.45 per term
Technologie de L'Information – Sécurité Informatique (MTCU 63002)	La Cité Collégiale	Domestic: $1775.37 International: $6016.76 (Fall 2015)	Domestic: $800.00 International: $800.00
Computer Systems Technology (MTCU 60505)	Fanshawe College	Domestic: $1383.16 International: $6180.00 (Fall 2015)	Domestic: $567.70 mandatory fees; $50.00 additional program fees, $206.29 co-op fees; general expenses vary $256.00-$1879.00 per term International: $840.70 mandatory fees; $50.00 additional program fees, $206.29 co-op fees; general expenses vary $256.00-$1879.00 per term
Computer Programmer Analyst (MTCU 60503)	Fanshawe College	Domestic: $1383.16 International: $6180.00 (Fall 2015)	Domestic: $567.70 mandatory fees; $50.00 additional program fees, $206.29 co-op fees; general expenses vary $160.00-$1614.00 per term International: $840.70 mandatory fees; $50.00 additional program fees, $206.29 co-op fees; general expenses vary $160.00-$1614.00 per term

6.5 Program Resources

a) **Capital requirements**

1. Specify the capital requirements required for startup of all levels.
2. Estimate the capital requirements for ongoing delivery of the program (up to the 5th year).
3. Specify the amount of capital investment required to implement this program that is beyond your existing capital allotment. If this exceeds $1.5 Million, also the source of these funds.
4. Specify the type of equipment and infrastructure enhancements needed to operationalize delivery of the program (electrical upgrade, water, eye wash station, fume hood, etc.).
5. Identify special lab amenities/attributes (functional requirements noted in 6.5 a) that impact 6.5 b)).

Consultation: Faculty, Chair, Program/Ops Manager, HS&S, Facilities Management

With the significant growth that the School of Information Technology is currently experiencing, there is not enough space in the existing network lab to accommodate this and other future programming. Currently, there are three additional programs that will require use of a network lab: one Graduate certificate starting in January (Network Security Architecture) and two in programs in development in Stage Gate 2 (IT Systems Operations and Digital Forensics). To allow for additional future growth and new program development, another networking/security lab will be required. The capital expenses should be shared between the new and existing programs that will make use of the new networking/security lab.

This program will require new equipment for the networking/security lab, including additional routers, switches, desktop computers, firewalls, security tools and software as well as forensic data gear. The lab space will also need to be cabled for an isolated network, isolated data centre and storage infrastructure, laptop use and wireless, and the equipment portion will need to be cooled/ventilated sufficiently for the network and server infrastructure equipment. The lab will be required for the launch of the program. As well, a DMZ will need to be implemented specifically for collaborative research opportunities with other universities.

b) **Space requirements**

See ***Appendix G: Detailed Course Delivery***

1. Will this program require renovations to existing space? If yes, describe.
2. Will this program require additional space? If yes, describe.
3. Will this program require designated space? If yes, describe.
4. Specify the size, type and attributes of classrooms and/or dedicated labs.

Consultation: Facilities Management, Timetabling/Scheduling

This program will require that new facilities be built in the form of two security/networking labs. The labs will need to be approximately 2,500 square feet in order to hold a maximum of 40 students and security, data centre and networking equipment. For additional courses, the program will make use of existing classrooms including laptop-enabled classrooms.

This network and security lab space will need to be designated as the primary lab for this Cyber Security program because the majority of the courses will need to be taught in the lab to utilize the equipment, which will be isolated from the College network, for hands-on labs and assignments. Due to high lab utilization of the existing network lab, additional courses will be placed in this space on an as-needed basis.

Discussions with Timetabling and Facilities are on-going. Lisa Dennis, Academic Support Coordinator with Academic Excellence and Innovation, has conducted a preliminary analysis of the usage of the existing specialty labs (G2010 and G2013), which supports the need for additional laboratory space to accommodate the new program (Please review Appendix G for details about the courses that will require the use of a networking lab):

Specialty Networking Labs Usage - G2010, G2013

for '15F and '16W; 40-seat labs
new programs - 1 section each

Lab Hours					**Year 1**		**Year 2**		**Year 3**		**Year 4**
Rooms	15F	16W	16F	17W	17F	18W	18F	19W	19F	20W	20F
G2010	48	54	48	54	48	54	48	54	48	54	48
G2013	56	48	56	48	56	48	56	48	56	48	56
New Hours - Grad Cert (F/W intakes)					8	16	16	16	16	16	16
New Hours - Adv Diploma (F/W intakes)					8	21	28	21	28	37	58
Total Hours	104	102	104	102	120	139	148	139	148	155	178
# Rooms Required at 80%	2.24	2.20	2.24	2.20	2.59	3.00	3.19	3.00	3.19	3.34	3.84
# Rooms Required at 60%	2.99	2.93	2.99	2.93	3.45	3.99	4.25	3.99	4.25	4.45	5.11

**assumed same hours in G2010/G2013 going forward as current hours; programs are CTY, CTN, ISM*
***did not include Summer hours*

c) **Computing requirements**

1. Identify any computers or related hardware devices that are to be funded:

   ☒ Desktop Computer ☐ Laptop ☐ Notebook ☐ Tablet

   ☐ PC based ☐ MAC ☐ IOS ☐ Android ☐ Other:

2. Identify any connectivity requirements that are to be funded:

   ☒ Permanent Hardwire ☒ Pluggable e.g. Laptop ☒ Wireless

   ☐ Other:

3. Identify any data storage requirements that are to be funded (excluding FOL):

   ☐ Local Hard Drive ☐ Area Server ☐ Central Server ☐ Cloud

   ☒ Other:

   - This program will require a small data store, with DMZ-accessible partitions/LUNS

4. Identify any software requirements and version:

☒ Office Professional Plus ☐ Office Project Professional

☐ Office Proof ☐ English ☐ French ☐ Spanish

☐ Office Publisher ☒ Office Visio

☐ Silverlight

☒ Other: software as yet to be determined

5. Estimate the computing requirements required for startup of all levels.
6. Estimate the computing requirements for ongoing delivery of the program (up to the 5th year).
7. What are the implications for existing IT architecture given program size, delivery format and computing requirements?
8. Does existing IT infrastructure allow this program to be offered as proposed? If no, what is required?
9. What are the software licensing fees (one time and annual)?
10. Is there a requirement to purchase enabling technologies (clickers, SMART Boards, etc.)? If yes, describe.
11. Can the proposed hardware and software run on the College's networks? If no, describe what is required.
12. What are the online registration, e-learning and FOL requirements?
13. Are there specific IT staff support needs for the program? If yes, describe.

Consultation: Information Technology Services

There are no known implications for the existing IT architecture given the program size, delivery format and computing requirements. The networking /security lab would exist in isolation from the College network.

There are no additional software requirements other than the **Connect fee**. It would be mandatory for all students to purchase their own laptop. Most courses will utilize open source tools and virtual machines, however there may be some additional tools, software and equipment that would enhance the learning of the students.

A front facing SMART board/tablet, digitally enabled teaching podium and a hi-res Video Digital Projector are recommended for use in the new security lab for instructional purposes.

The college networks would not be impacted by this program as it is required that the new security lab be separated from the College's network due to the nature of the activities that students will be performing in their labs. Where prudent, software will mostly be run on students' laptops using virtual environments.

In keeping with the e-learning policy of the college, all courses will have an e-learning component that will be accessed through Fanshawe Online.

The increased infrastructure and School of IT enrollment may require additional IT staff support hours to facilitate this program.

d) **Learning Resources -** Include collections and/or online resources required.
Consultation: Library

No additional resources will be needed from the Library. Resources currently available to students in the School of Information Technology's existing programs are sufficient.

e) **Marketing Plan** - Outline marketing strategies that will assist in reaching the appropriate student populations for this program.
Consultation: Reputation and Brand Management

Reputation and Brand Management recruiters will promote this new program when recruiting direct-entry, domestic students through the normal recruitment cycle. That will include high school visits, recruitment fairs, view book publications, and website and social media campaigns. Digital and traditional marketing campaigns including zap banners, radio, posters, print ads as well as Google AdWords will also be launched. The Fanshawe Open House and College Information Fair will also be used to recruit students into the program. This program will be targeting marketing campaigns in both the traditional catchment areas as well as throughout Ontario with a focus in the GTA.

Additional, more targeted promotion may be possible with the introduction of Specialist High Skills Major programs and dual credit courses in collaboration with the Thames Valley District School Board.

The International office will also be recruiting international students to this program through the use of in-country recruitment agents and local visits to target countries such as India and Nigeria.

6.6 Budget for Program - (multi-year) → See ***Appendix H: Multi-Year Budget Projections with Net Present Value (NPV).***

a) Quantify any estimated spending requirements that are above your existing budget.
b) Outline any budgetary assumptions.
c) What was the outcome of your funding calculation?
Consultation: Financial Planning

a) and b) Estimated Spending Requirements and Budgetary Assumptions :

- Two full-time faculty members and one coordinator position will be required; the remainder of the courses will be delivered by part-time and partial load faculty members.
- $50,000 has been allotted for faculty training for certification exams including the cost of training courses, travel, and exam fees.
- $72,000 has been estimated for curriculum development
- $440,000 has been estimated for equipment costs including consulting and installation in Year 1 and Year 3.
- $10,000 has been estimated for marketing expenses.
- Tuition and grant values are based on the amounts for the existing Advanced Diploma programs in the School of IT.

- The “Enrollment Tables” for each year of input data summarize enrollment numbers by semester for multiple cohorts/levels based on a Fall and a Winter intake each year.

c) The NPV @ 8% is $5,810,720.

6.7 Alternative Sources of Funding

a) Are there alternative sources of funding for this program (*e.g.*, donations, repurposing, partnerships)?

Consultation: Advancement and Alumni Office

No additional sources of funding have been identified at this time, but opportunities will continue to be explored.

Ontario College Quality Assurance Service
Service de l'assurance de la qualité des collèges de l'Ontario

APPLICATION FORM FOR PROGRAM PROPOSAL

A. Funding Request: This proposal will be sent to the MTCU for Approval for Funding.
☒Yes
☐No

B. College Name: Fanshawe College

C. College Contact(s): Person responsible for this proposal.

Name: Tracy Gedies
Title: Director, Centre for Academic Excellence
Telephone: 519-452-4430 ext. 4733
E-mail: tgedies@fanshawec.ca

Name: Jim Edwards
Title: Chair, School of Information Technology
Telephone: 519-452-4430 ext. 4629
E-mail: jwedwards@fanshawec.ca

D. Proposed Program Title: Cyber Security

E. Proposed Credential: Please select one (1).
☐Local Board Approved Certificate
☐Ontario College Certificate
☐Ontario College Diploma
☒Ontario College Advanced Diploma
☐Ontario College Graduate Certificate

F. Program Maps (Appendix A): Please complete and attach the two (2) Program Maps.
Form 1- Vocational Program Learning Outcomes
Form 2- Essential Employability Skills Outcomes

G. Program Description (Appendix B): Please complete and attach the Program Description Form.

H. Program Curriculum (Appendix C): Please complete and attach the Program Curriculum Form.

I. Regulatory Status Form (Appendix D): Please complete and attach the Regulatory Status Form.

J. Date of Submission to CVS: Click here to enter a date.

FOR CVS USE ONLY

K. Date of CVS Response: Click here to enter a date.

L. CVS Validation Decision:
☐Proposal Validated. APS Number:
Reason:
☐Proposal not Validated.
Reason:

M. CVS Signature:

Send the completed form and required appendices to: belfer@ocqas.org. For detailed information on how to complete the *Application Form for Program Proposal*, please refer to the *Instructions for Submission of Program Proposal* document at www.ocqas.org.

INTRODUCTION

The process established by the Credentials Validation Service (CVS) is designed to be a streamlined, seamless, effective, and efficient process that will allow colleges to submit and receive validation requests and decisions in a timely manner. The document with the instructions to complete this form (*CVS Instructions for Submission of Program Proposal*) is available to all colleges on the OCQAS website (www.ocqas.org).

F. PROGRAM MAPS (APPENDIX A): Form 1 - Vocational Program Learning Outcomes

Provincial Vocational Program Outcomes ☐ Provincial Program Standard, *or* ☒ Provincial Program Description *MTCU code*: MTCU 73002	**Proposed Program Vocational Learning Outcomes (for MTCU 63002)**	**Course Title / Course Code**
1. Recommend ideal security solutions considering the affordances and limitations of the computer operating systems, networks, application software, and packages available.	1. Configure, implement, and manage security devices and equipment considering the unique features of the computer operating systems, networks, applications and software.	INFO-1135 Networking Fundamentals INFO-1150 Programming Fundamentals INFO-1120 Database Fundamentals INFO-1178 Configuring Windows Client INFO-XXXX Network Components INFO-XXXX PHP Fundamentals INFO-1124 Computer Security Concepts INFO-XXXX Cryptography & Authentication Systems INFO-XXXX Introduction to Unix INFO-XXXX Securing Windows Systems INFO-XXXX Web Security INFO-XXXX Wireless and Mobile INFO-XXXX Network Protocols INFO-XXXX Security Mechanisms INFO-XXXX Digital Forensics INFO-XXXX Secure Scripting and Automation INFO-XXXX LAMP Security INFO-XXXX Network Monitoring and Change Management INFO-XXXX Evolving Technologies and Threats

		INFO-XXXX Computational Intelligence INFO-XXXX Perimeter Defense and Design INFO-XXXX Attack Vectors and Analysis INFO-XXXX Penetration Testing INFO-XXXX Incidence Handling and Response INFO-XXXX Technical Writing and Presentation INFO-XXXX Research Project & Entrepreneurship INFO-XXXX Hacking Techniques and Exploits INFO-XXXX Advanced Penetration Testing INFO-XXXX Secure Network Architecture
2. Validate security solution designs for business processes and applications to secure business data. 3. Recommend the processes and procedures for deployment of security solutions. 4. Select security strategies for business communications that respond to the needs of all the internal stakeholders.	2. Implement and evaluate security solutions for business processes, applications and communications to protect business resources and respond to the needs of all the internal stakeholders.	INFO-1135 Networking Fundamentals INFO-1150 Programming Fundamentals INFO-1120 Database Fundamentals INFO-1178 Configuring Windows Client INFO-XXXX Network Components INFO-XXXX PHP Fundamentals INFO-1124 Computer Security Concepts INFO-XXXX Cryptography & Authentication Systems INFO-XXXX Introduction to Unix INFO-XXXX Securing Windows Systems INFO-XXXX Security Management INFO-XXXX Web Security INFO-XXXX Wireless and Mobile INFO-XXXX Network Protocols INFO-XXXX Security Mechanisms

		INFO-XXXX Secure Scripting and Automation INFO-XXXX LAMP Security INFO-XXXX Network Monitoring and Change Management INFO-XXXX Auditing and Security Controls INFO-XXXX Evolving Technologies and Threats INFO-XXXX Perimeter Defense and Design INFO-XXXX Attack Vectors and Analysis INFO-XXXX Penetration Testing INFO-XXXX Incidence Handling and Response INFO-XXXX Technical Writing and Presentation INFO-5096 Managing & Budgeting Technical Projects INFO-XXXX Research Project & Entrepreneurship INFO-XXXX Secure Network Architecture
6. Produce project management to effectively respond to the needs of the organization's information security requirements.	3. Use project management principles to implement security strategies and processes that address the organization's information security requirements.	INFO-1124 Computer Security Concepts INFO-XXXX Security Management INFO-XXXX Network Monitoring and Change Management INFO-XXXX Auditing and Security Controls INFO-XXXX Technical Writing and Presentation INFO-5096 Managing & Budgeting Technical Projects INFO-XXXX Research Project & Entrepreneurship INFO-XXXX Malware Analysis and Response

5. Revise security solutions to align with policies, standards, and regulations within the organization. 8. Develop appropriate internal security training to ensure compliance with security policies. 9. Recommend security protocols, policies, audit results and related documentation for communication to any level of the organization. 13. Communicate effectively with all staff and management in the workplace.	4. Develop, implement and evaluate organizational security policies, standards and regulations to promote internal security.	INFO-1135 Networking Fundamentals INFO-1150 Programming Fundamentals INFO-1120 Database Fundamentals INFO-1178 Configuring Windows Client INFO-XXXX Network Components INFO-XXXX PHP Fundamentals INFO-1124 Computer Security Concepts INFO-XXXX Cryptography & Authentication Systems INFO-XXXX Introduction to Unix INFO-XXXX Securing Windows Systems INFO-XXXX Security Management INFO-XXXX Web Security INFO-XXXX Wireless and Mobile INFO-XXXX Network Protocols INFO-XXXX Security Mechanisms INFO-XXXX Digital Forensics INFO-XXXX Secure Scripting and Automation INFO-XXXX LAMP Security INFO-XXXX Network Monitoring and Change Management INFO-XXXX Auditing and Security Controls INFO-XXXX Evolving Technologies and Threats INFO-XXXX Computational Intelligence INFO-XXXX Perimeter Defense and Design INFO-XXXX Attack Vectors and Analysis INFO-XXXX Penetration Testing INFO-XXXX Incidence Handling and Response

		INFO-XXXX Technical Writing and Presentation INFO-XXXX Research Project & Entrepreneurship INFO-XXXX Secure Network Architecture

10. Select appropriate procedures to mitigate how intruders escalate privileges and what steps can be taken to secure a system. 12. Manage network security through practical work applications.	5. Perform vulnerability assessments and penetration testing for infrastructures, web and applications, using both manual and automated techniques.	INFO-1150 Programming Fundamentals INFO-1124 Computer Security Concepts INFO-XXXX Securing Windows Systems INFO-XXXX Security Management INFO-XXXX Network Monitoring and Change Management INFO-XXXX Auditing and Security Controls INFO-XXXX Perimeter Defense and Design INFO-XXXX Attack Vectors and Analysis INFO-XXXX Penetration Testing INFO-XXXX Incidence Handling and Response INFO-XXXX Technical Writing and Presentation INFO-XXXX Research Project & Entrepreneurship INFO-XXXX Hacking Techniques and Exploits INFO-XXXX Advanced Penetration Testing
11. Integrate ethical hacking techniques to formulate countermeasures designed to secure information systems against system threats.	6. Evaluate and apply tools and techniques to formulate countermeasures to secure information systems against security threats.	INFO-XXXX Network Components INFO-XXXX PHP Fundamentals INFO-1124 Computer Security Concepts INFO-XXXX Cryptography & Authentication Systems INFO-XXXX Securing Windows Systems INFO-XXXX Security Management INFO-XXXX Web Security INFO-XXXX Wireless and Mobile

		INFO-XXXX Network Protocols INFO-XXXX Security Mechanisms INFO-XXXX Digital Forensics INFO-XXXX Secure Scripting and Automation INFO-XXXX LAMP Security INFO-XXXX Network Monitoring and Change Management INFO-XXXX Auditing and Security Controls INFO-XXXX Evolving Technologies and Threats INFO-XXXX Computational Intelligence INFO-XXXX Perimeter Defense and Design INFO-XXXX Attack Vectors and Analysis INFO-XXXX Penetration Testing INFO-XXXX Incidence Handling and Response INFO-XXXX Technical Writing and Presentation INFO-XXXX Research Project & Entrepreneurship INFO-XXXX Hacking Techniques and Exploits INFO-XXXX Advanced Penetration Testing
2. Validate security solution designs for business processes and applications to secure business data. 3. Recommend the processes and procedures for deployment of security solutions. 7. Evaluate the effectiveness of a security system through security audits to identify and correct security issues.	7. Perform security audits and forensic analysis to evaluate the effectiveness of a security system, and identify and correct security vulnerabilities.	CRIM-XXXX Cybercrime INFO-XXXX Security Management INFO-XXXX Security Mechanisms INFO-XXXX Digital Forensics INFO-XXXX Network Monitoring and Change Management INFO-XXXX Auditing and Security Controls

		INFO-XXXX Perimeter Defense and Design INFO-XXXX Attack Vectors and Analysis INFO-XXXX Penetration Testing INFO-XXXX Incidence Handling and Response INFO-XXXX Technical Writing and Presentation INFO-XXXX Research Project & Entrepreneurship
12. Manage network security through practical work applications.	8. Monitor and analyze logs and alerts from security devices to determine the extent of a security breach and what data has been compromised.	INFO-1135 Networking Fundamentals INFO-XXXX Security Management INFO-XXXX Wireless and Mobile INFO-XXXX Network Protocols INFO-XXXX Security Mechanisms INFO-XXXX Digital Forensics INFO-XXXX Secure Scripting and Automation INFO-XXXX LAMP Security INFO-XXXX Network Monitoring and Change Management INFO-XXXX Auditing and Security Controls INFO-XXXX Perimeter Defense and Design INFO-XXXX Attack Vectors and Analysis INFO-XXXX Penetration Testing INFO-XXXX Incidence Handling and Response INFO-XXXX Technical Writing and Presentation INFO-XXXX Research Project & Entrepreneurship

		INFO-XXXX Secure Network Architecture
Extension outside of business/company of 9. Recommend security protocols, policies, audit results and related documentation for communication to any level of the organization. 13. Communicate effectively with all staff and management in the workplace.	9. Identify, collect and log relevant data as evidence for a sample case within a business or in the Canadian Justice System.	PHIL-XXXX Ethics INFO-1124 Computer Security Concepts CRIM-XXXX Cybercrime INFO-XXXX Security Mechanisms INFO-XXXX Digital Forensics INFO-XXXX Network Monitoring and Change Management INFO-XXXX Auditing and Security Controls INFO-XXXX Computational Intelligence CRIM-3001 Criminology INFO-XXXX Attack Vectors and Analysis INFO-XXXX Technical Writing and Presentation INFO-XXXX Research Project & Entrepreneurship INFO-XXXX Hacking Techniques and Exploits

Add additional rows as required to complete the mapping exercise.

F. PROGRAM MAPS (APPENDIX A): Form 2 – Essential Employability Skills Outcomes

Skill Categories	**Defining Skills** Skill areas to be demonstrated by the graduates	**Essential Employability Skills Outcomes** The graduate has reliably demonstrated the ability to:	**Course Title / Course Codes** (*As indicated in Appendix A*)
Communication	• Reading • Writing • Speaking • Listening • Presenting • Visual Literacy	• communicate clearly, concisely, and correctly in the written, spoken, and visual form that fulfils the purpose and meets the needs of the audience	INFO-1135 Networking Fundamentals INFO-1150 Programming Fundamentals INFO-1120 Database Fundamentals INFO-1178 Configuring Windows Client PHIL-XXXX Ethics WRIT-1043 Reasoning & Writing 1 for IT OR WRIT-1034 Reasoning & Writing 1 – EAP INFO-XXXX Network Components INFO-XXXX PHP Fundamentals INFO-1124 Computer Security Concepts INFO-XXXX Cryptography & Authentication Systems INFO-XXXX Introduction to Unix CRIM-XXXX Cybercrime INFO-XXXX Securing Windows Systems COMM-3047 Communication for IT Professionals COOP-1020 Co-operative Education Employment Preparation

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
			INFO-XXXX Security Management INFO-XXXX Web Security INFO-XXXX Wireless and Mobile INFO-XXXX Network Protocols INFO-XXXX Security Mechanisms INFO-XXXX Digital Forensics INFO-XXXX Secure Scripting and Automation INFO-XXXX LAMP Security INFO-XXXX Network Monitoring and Change Management INFO-XXXX Auditing and Security Controls INFO-XXXX Evolving Technologies and Threats INFO-XXXX Computational Intelligence CRIM-3001 Criminology INFO-XXXX Perimeter Defense and Design INFO-XXXX Attack Vectors and Analysis INFO-XXXX Penetration Testing INFO-XXXX Incidence Handling and Response INFO-XXXX Technical Writing and Presentation BUSI-XXXX Entrepreneurship and Project Management

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
			INFO-XXXX Research Project & Entrepreneurship INFO-XXXX Hacking Techniques and Exploits INFO-XXXX Advanced Penetration Testing INFO-XXXX Malware Analysis and Response INFO-XXXX Secure Network Architecture
		• respond to written, spoken, or visual messages in a manner that ensures effective communication	INFO-1135 Networking Fundamentals INFO-1178 Configuring Windows Client PHIL-XXXX Ethics WRIT-1043 Reasoning & Writing 1 for IT OR WRIT-1034 Reasoning & Writing 1 – EAP INFO-XXXX Network Components INFO-1124 Computer Security Concepts INFO-XXXX Cryptography & Authentication Systems INFO-XXXX Introduction to Unix CRIM-XXXX Cybercrime INFO-XXXX Securing Windows Systems COMM-3047 Communication for IT Professionals

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
			COOP-1020 Co-operative Education Employment Preparation INFO-XXXX Security Management INFO-XXXX Web Security INFO-XXXX Wireless and Mobile INFO-XXXX Network Protocols INFO-XXXX Security Mechanisms INFO-XXXX Digital Forensics INFO-XXXX LAMP Security INFO-XXXX Network Monitoring and Change Management INFO-XXXX Auditing and Security Controls INFO-XXXX Evolving Technologies and Threats INFO-XXXX Computational Intelligence CRIM-3001 Criminology INFO-XXXX Perimeter Defense and Design INFO-XXXX Attack Vectors and Analysis INFO-XXXX Penetration Testing INFO-XXXX Incidence Handling and Response INFO-XXXX Technical Writing and Presentation INFO-5096 Managing & Budgeting Technical

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
			Projects INFO-XXXX Research Project & Entrepreneurship INFO-XXXX Hacking Techniques and Exploits INFO-XXXX Advanced Penetration Testing INFO-XXXX Malware Analysis and Response INFO-XXXX Secure Network Architecture
Numeracy	• Understanding and applying mathematical concepts and reasoning • Analysing and using numerical data • Conceptualizing	• execute mathematical operations accurately	INFO-1135 Networking Fundamentals INFO-1150 Programming Fundamentals INFO-1120 Database Fundamentals INFO-1178 Configuring Windows Client INFO-XXXX Network Components INFO-XXXX PHP Fundamentals INFO-XXXX Cryptography & Authentication Systems INFO-XXXX Introduction to Unix CRIM-XXXX Cybercrime INFO-XXXX Securing Windows Systems INFO-XXXX Security Management INFO-XXXX Web Security INFO-XXXX Network Protocols

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
			INFO-XXXX Secure Scripting and Automation INFO-XXXX LAMP Security INFO-XXXX Network Monitoring and Change Management INFO-XXXX Auditing and Security Controls INFO-XXXX Evolving Technologies and Threats INFO-XXXX Computational Intelligence INFO-XXXX Perimeter Defense and Design INFO-XXXX Attack Vectors and Analysis INFO-XXXX Penetration Testing INFO-XXXX Incidence Handling and Response INFO-5096 Managing & Budgeting Technical Projects INFO-XXXX Research Project & Entrepreneurship INFO-XXXX Hacking Techniques and Exploits INFO-XXXX Advanced Penetration Testing INFO-XXXX Malware Analysis and Response INFO-XXXX Secure Network Architecture
Critical Thinking & Problem	• Analysing • Synthesizing	• apply a systematic approach to solve problems	INFO-1135 Networking Fundamentals INFO-1150 Programming Fundamentals INFO-1120 Database Fundamentals

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
Solving	• Evaluating • Decision-making • Creative and innovative thinking		INFO-1178 Configuring Windows Client WRIT-1043 Reasoning & Writing 1 for IT OR WRIT-1034 Reasoning & Writing 1 – EAP INFO-XXXX Network Components INFO-XXXX PHP Fundamentals INFO-XXXX Cryptography & Authentication Systems INFO-XXXX Introduction to Unix CRIM-XXXX Cybercrime INFO-XXXX Securing Windows Systems COMM-3047 Communication for IT Professionals INFO-XXXX Security Management INFO-XXXX Web Security INFO-XXXX Network Protocols INFO-XXXX Security Mechanisms INFO-XXXX Digital Forensics INFO-XXXX Secure Scripting and Automation INFO-XXXX LAMP Security INFO-XXXX Network Monitoring and Change Management

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
			INFO-XXXX Auditing and Security Controls INFO-XXXX Evolving Technologies and Threats INFO-XXXX Computational Intelligence CRIM-3001 Criminology INFO-XXXX Perimeter Defense and Design INFO-XXXX Attack Vectors and Analysis INFO-XXXX Penetration Testing INFO-XXXX Incidence Handling and Response INFO-XXXX Technical Writing and Presentation INFO-5096 Managing & Budgeting Technical Projects INFO-XXXX Research Project & Entrepreneurship INFO-XXXX Hacking Techniques and Exploits INFO-XXXX Advanced Penetration Testing INFO-XXXX Malware Analysis and Response INFO-XXXX Secure Network Architecture
		• use a variety of thinking skills to anticipate and solve problems	INFO-1135 Networking Fundamentals INFO-1150 Programming Fundamentals INFO-1120 Database Fundamentals INFO-1178 Configuring Windows Client

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
			WRIT-1043 Reasoning & Writing 1 for IT OR WRIT-1034 Reasoning & Writing 1 – EAP INFO-XXXX Network Components INFO-XXXX PHP Fundamentals INFO-XXXX Cryptography & Authentication Systems INFO-XXXX Introduction to Unix CRIM-XXXX Cybercrime INFO-XXXX Securing Windows Systems COMM-3047 Communication for IT Professionals INFO-XXXX Security Management INFO-XXXX Web Security INFO-XXXX Wireless and Mobile INFO-XXXX Network Protocols INFO-XXXX Security Mechanisms INFO-XXXX Digital Forensics INFO-XXXX Secure Scripting and Automation INFO-XXXX LAMP Security INFO-XXXX Network Monitoring and Change

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
			Management INFO-XXXX Auditing and Security Controls INFO-XXXX Evolving Technologies and Threats INFO-XXXX Computational Intelligence CRIM-3001 Criminology INFO-XXXX Perimeter Defense and Design INFO-XXXX Attack Vectors and Analysis INFO-XXXX Penetration Testing INFO-XXXX Incidence Handling and Response INFO-XXXX Technical Writing and Presentation INFO-5096 Managing & Budgeting Technical Projects INFO-XXXX Research Project & Entrepreneurship INFO-XXXX Hacking Techniques and Exploits INFO-XXXX Advanced Penetration Testing INFO-XXXX Malware Analysis and Response INFO-XXXX Secure Network Architecture
Information Management	• Gathering and managing information	• locate, select, organize, and document information using appropriate technology and	INFO-1135 Networking Fundamentals INFO-1150 Programming Fundamentals INFO-1120 Database Fundamentals

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
	• Selecting and using appropriate tools and technology for a task or a project • Computer literacy • Internet skills	information systems	INFO-1178 Configuring Windows Client PHIL-XXXX Ethics WRIT-1043 Reasoning & Writing 1 for IT OR WRIT-1034 Reasoning & Writing 1 – EAP INFO-XXXX Network Components INFO-XXXX PHP Fundamentals INFO-XXXX Cryptography & Authentication Systems INFO-XXXX Introduction to Unix CRIM-XXXX Cybercrime INFO-XXXX Securing Windows Systems COMM-3047 Communication for IT Professionals COOP-1020 Co-operative Education Employment Preparation INFO-XXXX Security Management INFO-XXXX Web Security INFO-XXXX Wireless and Mobile INFO-XXXX Network Protocols INFO-XXXX Digital Forensics INFO-XXXX Secure Scripting and Automation

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
			INFO-XXXX LAMP Security INFO-XXXX Network Monitoring and Change Management INFO-XXXX Auditing and Security Controls INFO-XXXX Evolving Technologies and Threats INFO-XXXX Computational Intelligence CRIM-3001 Criminology INFO-XXXX Perimeter Defense and Design INFO-XXXX Attack Vectors and Analysis INFO-XXXX Penetration Testing INFO-XXXX Incidence Handling and Response INFO-XXXX Technical Writing and Presentation INFO-5096 Managing & Budgeting Technical Projects INFO-XXXX Research Project & Entrepreneurship INFO-XXXX Hacking Techniques and Exploits INFO-XXXX Advanced Penetration Testing INFO-XXXX Malware Analysis and Response INFO-XXXX Secure Network Architecture
		• analyse, evaluate, and apply relevant	INFO-1135 Networking Fundamentals

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
		information from a variety of sources	INFO-1150 Programming Fundamentals INFO-1120 Database Fundamentals INFO-1178 Configuring Windows Client PHIL-XXXX Ethics WRIT-1043 Reasoning & Writing 1 for IT OR WRIT-1034 Reasoning & Writing 1 – EAP INFO-XXXX Network Components INFO-XXXX PHP Fundamentals INFO-XXXX Cryptography & Authentication Systems INFO-XXXX Introduction to Unix CRIM-XXXX Cybercrime INFO-XXXX Securing Windows Systems COMM-3047 Communication for IT Professionals COOP-1020 Co-operative Education Employment Preparation INFO-XXXX Security Management INFO-XXXX Web Security INFO-XXXX Wireless and Mobile INFO-XXXX Network Protocols INFO-XXXX Digital Forensics

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
			INFO-XXXX Secure Scripting and Automation INFO-XXXX LAMP Security INFO-XXXX Network Monitoring and Change Management INFO-XXXX Auditing and Security Controls INFO-XXXX Evolving Technologies and Threats INFO-XXXX Computational Intelligence CRIM-3001 Criminology INFO-XXXX Perimeter Defense and Design INFO-XXXX Attack Vectors and Analysis INFO-XXXX Penetration Testing INFO-XXXX Incidence Handling and Response INFO-XXXX Technical Writing and Presentation INFO-5096 Managing & Budgeting Technical Projects INFO-XXXX Research Project & Entrepreneurship INFO-XXXX Hacking Techniques and Exploits INFO-XXXX Advanced Penetration Testing INFO-XXXX Malware Analysis and Response

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
			INFO-XXXX Secure Network Architecture
Inter-personal	• Team work • Relationship management • Conflict resolution • Leadership • Networking	• show respect for the diverse opinions, values, belief systems, and contributions of others	INFO-1135 Networking Fundamentals INFO-1150 Programming Fundamentals INFO-1120 Database Fundamentals INFO-1178 Configuring Windows Client PHIL-XXXX Ethics WRIT-1043 Reasoning & Writing 1 for IT OR WRIT-1034 Reasoning & Writing 1 – EAP INFO-XXXX Network Components INFO-XXXX PHP Fundamentals INFO-XXXX Cryptography & Authentication Systems INFO-XXXX Introduction to Unix CRIM-XXXX Cybercrime INFO-XXXX Securing Windows Systems COMM-3047 Communication for IT Professionals COOP-1020 Co-operative Education Employment Preparation INFO-XXXX Security Management INFO-XXXX Web Security INFO-XXXX Wireless and Mobile

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
			INFO-XXXX Network Protocols INFO-XXXX Digital Forensics INFO-XXXX Secure Scripting and Automation INFO-XXXX LAMP Security INFO-XXXX Network Monitoring and Change Management INFO-XXXX Auditing and Security Controls INFO-XXXX Computational Intelligence CRIM-3001 Criminology INFO-XXXX Perimeter Defense and Design INFO-XXXX Attack Vectors and Analysis INFO-XXXX Penetration Testing INFO-XXXX Incidence Handling and Response INFO-XXXX Technical Writing and Presentation INFO-5096 Managing & Budgeting Technical Projects INFO-XXXX Research Project & Entrepreneurship INFO-XXXX Hacking Techniques and Exploits INFO-XXXX Advanced Penetration Testing INFO-XXXX Malware Analysis and Response

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
			INFO-XXXX Secure Network Architecture
		• interact with others in groups or teams in ways that contribute to effective working relationships and the achievement of goals	INFO-1135 Networking Fundamentals INFO-1150 Programming Fundamentals INFO-1120 Database Fundamentals WRIT-1043 Reasoning & Writing 1 for IT OR WRIT-1034 Reasoning & Writing 1 – EAP INFO-XXXX Network Components INFO-XXXX PHP Fundamentals INFO-1124 Computer Security Concepts INFO-XXXX Cryptography & Authentication Systems INFO-XXXX Introduction to Unix CRIM-XXXX Cybercrime INFO-XXXX Securing Windows Systems COMM-3047 Communication for IT Professionals COOP-1020 Co-operative Education Employment Preparation INFO-XXXX Security Management INFO-XXXX Web Security INFO-XXXX Wireless and Mobile INFO-XXXX Network Protocols

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
			INFO-XXXX Security Mechanisms INFO-XXXX Digital Forensics INFO-XXXX Secure Scripting and Automation INFO-XXXX LAMP Security INFO-XXXX Network Monitoring and Change Management INFO-XXXX Auditing and Security Controls INFO-XXXX Computational Intelligence CRIM-3001 Criminology INFO-XXXX Perimeter Defense and Design INFO-XXXX Attack Vectors and Analysis INFO-XXXX Penetration Testing INFO-XXXX Incidence Handling and Response INFO-XXXX Technical Writing and Presentation INFO-5096 Managing & Budgeting Technical Projects INFO-XXXX Research Project & Entrepreneurship INFO-XXXX Hacking Techniques and Exploits INFO-XXXX Advanced Penetration Testing INFO-XXXX Malware Analysis and Response

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
			INFO-XXXX Secure Network Architecture
Personal	• Managing self • Managing change and being flexible and adaptable • Engaging in reflective practice • Demonstrating personal responsibility	• manage the use of time and other resources to complete projects	INFO-1135 Networking Fundamentals INFO-1150 Programming Fundamentals INFO-1120 Database Fundamentals INFO-1178 Configuring Windows Client WRIT-1043 Reasoning & Writing 1 for IT OR WRIT-1034 Reasoning & Writing 1 – EAP INFO-XXXX Network Components INFO-XXXX PHP Fundamentals INFO-1124 Computer Security Concepts INFO-XXXX Cryptography & Authentication Systems INFO-XXXX Introduction to Unix CRIM-XXXX Cybercrime INFO-XXXX Securing Windows Systems COMM-3047 Communication for IT Professionals COOP-1020 Co-operative Education Employment Preparation INFO-XXXX Security Management INFO-XXXX Web Security INFO-XXXX Wireless and Mobile

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
			INFO-XXXX Network Protocols INFO-XXXX Security Mechanisms INFO-XXXX Digital Forensics INFO-XXXX Secure Scripting and Automation INFO-XXXX LAMP Security INFO-XXXX Network Monitoring and Change Management INFO-XXXX Auditing and Security Controls INFO-XXXX Computational Intelligence CRIM-3001 Criminology INFO-XXXX Perimeter Defense and Design INFO-XXXX Attack Vectors and Analysis INFO-XXXX Penetration Testing INFO-XXXX Incidence Handling and Response INFO-XXXX Technical Writing and Presentation INFO-5096 Managing & Budgeting Technical Projects INFO-XXXX Research Project & Entrepreneurship INFO-XXXX Hacking Techniques and Exploits INFO-XXXX Advanced Penetration Testing

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
			INFO-XXXX Malware Analysis and Response INFO-XXXX Secure Network Architecture
		• take responsibility for one's own actions, decisions, and consequences	INFO-1135 Networking Fundamentals INFO-1150 Programming Fundamentals INFO-1120 Database Fundamentals INFO-1178 Configuring Windows Client PHIL-XXXX Ethics WRIT-1043 Reasoning & Writing 1 for IT OR WRIT-1034 Reasoning & Writing 1 – EAP INFO-XXXX Network Components INFO-XXXX PHP Fundamentals INFO-XXXX Cryptography & Authentication Systems INFO-XXXX Introduction to Unix CRIM-XXXX Cybercrime INFO-XXXX Securing Windows Systems COMM-3047 Communication for IT Professionals COOP-1020 Co-operative Education Employment Preparation INFO-XXXX Security Management INFO-XXXX Web Security

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
			INFO-XXXX Wireless and Mobile INFO-XXXX Network Protocols INFO-XXXX Security Mechanisms INFO-XXXX Digital Forensics INFO-XXXX Secure Scripting and Automation INFO-XXXX LAMP Security INFO-XXXX Network Monitoring and Change Management INFO-XXXX Auditing and Security Controls INFO-XXXX Computational Intelligence CRIM-3001 Criminology INFO-XXXX Perimeter Defense and Design INFO-XXXX Attack Vectors and Analysis INFO-XXXX Penetration Testing INFO-XXXX Incidence Handling and Response INFO-XXXX Technical Writing and Presentation INFO-5096 Managing & Budgeting Technical Projects INFO-XXXX Research Project & Entrepreneurship INFO-XXXX Hacking Techniques and Exploits

Skill Categories	Defining Skills Skill areas to be demonstrated by the graduates	Essential Employability Skills Outcomes The graduate has reliably demonstrated the ability to:	Course Title / Course Codes (*As indicated in Appendix A*)
			INFO-XXXX Advanced Penetration Testing INFO-XXXX Malware Analysis and Response INFO-XXXX Secure Network Architecture

G. PROGRAM DESCRIPTION (APPENDIX B)

Program Description

Provide a brief description of the program, similar to what might be used as, or found in, advertising or a calendar description.

This three-year Advanced Diploma in Cyber Security will provide students with the foundational Information Technology (IT) skills and knowledge necessary to be successful in the IT industry. Foundational topics will include network management/analysis, programming and scripting, operating systems, and database management. Building on those foundational topics, the curriculum will also develop students' skills in the areas of risk analysis, cryptography, vulnerability testing, access control implementation, and security audit performance. Graduates of this program will be able to proactively implement sound security practices to mitigate security risks and respond quickly to security breaches and issues that may have occurred. They will also have the foundational knowledge and skills required to write the certification exams for industry-recognized certifications from CompTIA, ISACA, CISSP, and Certified Ethical Hacker.

Through hands-on laboratory activities, case study analyses, and research projects, students will enhance their technical abilities and develop their interpersonal, communication, organizational, and problem-solving skills. This program will also include three co-operative education work placements to further enhance all of those skills.

This program will delivered face-to-face (web-facilitated).

Laddering Opportunities

Provide a brief description of known laddering into and from the proposed program, e.g. certificate to diploma, diploma to degree, apprenticeship to college, diploma to apprenticeship, college to college, diploma to college degree, etc.

Since there is enough overlap among the first semesters for this program, the Computer System Technician/Technology programs, and the Computer Programmer Analyst program, students will be able to transfer to or from any of these programs for the second semester. Upon completion of this Advanced Diploma, students will be able to further their education with a series of Graduate Certificates specializing in specific areas of IT Security (Information Systems Management, Network Security Architecture), Public Safety, or Business. These Graduate certificates would provide students with higher-level learning focusing on a specific program area in IT (e.g., security architecture, digital forensics, IT infrastructure management). Upon completion of a Graduate Certificate in a security-related field, students will be eligible to apply for the Master of Computing program at the University of Gloucestershire in the UK.

Occupational Areas

Provide a brief description of where it is anticipated graduates will find employment.

Graduates of this program will likely find employment as junior security analysts/specialists, network/systems managers/administrators/analysts, or network/systems/security support specialists.

Proposed Program Vocational Learning Outcomes

Provide the list of the proposed program vocational learning outcomes. These outcomes should be listed, verbatim as they appear in Appendix A- Form 1.

***The graduate has reliably demonstrated the ability to*:**

1. Configure, implement, and manage security devices and equipment considering the unique features of the computer operating systems, networks, applications and software.
2. Implement and evaluate security solutions for business processes, applications and communications to protect business resources and respond to the needs of all the internal stakeholders.
3. Use project management principles to implement security strategies and processes that address the organization's information security requirements.

4. Develop, implement and evaluate organizational security policies, standards and regulations to promote internal security.
5. Perform vulnerability assessments and penetration testing for infrastructures, web and applications, using both manual and automated techniques.
6. Evaluate and apply tools and techniques to formulate countermeasures to secure information systems against security threats.
7. Perform security audits and forensic analysis to evaluate the effectiveness of a security system, and identify and correct security vulnerabilities.
8. Monitor and analyze logs and alerts from security devices to determine the extent of a security breach and what data has been compromised.
9. Identify, collect and log relevant data as evidence for a sample case within a business or in the Canadian Justice System.

Admission Requirements

Identify the Admission Requirements for the program.

OSSD with courses from the College (C), University (U),
University/College (M), or Open (O) stream WITH:
- Any Grade 12 English (C) or (U)
- Any Grade 11 or Grade 12 Mathematics* (C), (U), or (M)

OR

Academic and Career Entrance Certificate (ACE)

OR

Ontario High School Equivalency Certificate (GED) AND:
- Any Grade 11 or Grade 12 Mathematics* (C), (U), or (M)

OR

Mature Applicant with standing in the required courses stated above

Note:
•*Applicants who lack the required Mathematics may still gain eligibility for admission by completing appropriate prior upgrading.

English Language Requirements

Applicants whose first language is not English will be required to demonstrate proficiency in English by one of the following methods:
•A Grade 12 College Stream or University Stream English credit from an Ontario Secondary School, or equivalent, depending on the program's Admission Requirements
•Test of English as a Foreign Language (TOEFL) test with a minimum score of 550 for the paper-based test (PBT), or 79 for the Internet-based test (iBT), with test results within the last two years
•International English Language Testing System (IELTS) test with an overall score of 6.0 with no score less than 5.5 in any of the four bands, with test results within the last two years
•Canadian Academic English Language (CAEL) test with an overall score of 60 with no score less than 50 in any of the four bands, with test results within the last two years
•An English Language Evaluation (ELE) at Fanshawe College with a minimum score of 70% in all sections of the test, with test results within the last two years

Recommended Academic Preparation

•Grade 12 Business and Technological Communication (O)
•Grade 11 and Grade 12 Computer Engineering Technology (M)
•Grade 11 Introduction to Computer Science (U)
•Grade 12 Computer Science (U)

•Grade 11 Information and Communication Technology: The Digital Environment (O)
•Grade 12 Information and Communication Technology: Multimedia Solutions (C)
•Academic and Career Entrance Certificate (ACE): Business or Technical Mathematics course and Computer Skills course

Applicant Selection Criteria
Where the number of eligible applicants exceeds the available spaces in the program, the Applicant Selection Criteria will be:
1.Preference for Permanent Residents of Ontario
2.Receipt of Application by February 1st (After this date, Fanshawe College will consider applicants on a first-come, first-served basis until the program is full)
3.Achievement in the Admission Requirements
- See more at: https://www.fanshawec.ca/programs-and-courses/program/cty1-computer-systems-technology/next-year#group_admission

H. PROGRAM CURRICULUM (APPENDIX C)

Semester	Course Code/ Course Title (*As indicated in Appendix A*)	General Education Course *(indicate with an X)*	Total Course Hours	Course Description
1	INFO-1135 Networking Fundamentals		75	This course provides students with a comprehensive overview of networking; from fundamentals to advanced applications, thereby providing a solid foundation upon which to build their Local Area Network (LAN) and Wide Area Network (WAN) training. It is based on a bottom-up approach to networking and emphasizes the concepts and skills required to design networks, while providing opportunities for practical application and hands-on experience by teaching students how to install, operate, and maintain networks.
1	INFO-1150 Programming Fundamentals		75	This course is an introduction to the fundamentals of procedural programming using the Java programming language. Although Java is an object-oriented language, the focus of the course will be on writing programs using the procedural programming approach. A problem solving approach towards programming will be emphasized throughout the course. Problem analysis and algorithmic thinking skills will be introduced to develop good program writing technique. The course will introduce the following programming concepts: data types, creating and referencing variables, the three procedural programming concepts of sequence, selection , and repetition, data input validation, simple testing and bug hunting techniques, coding using methods, and using arrays and arrayLists as data storage structures. Students will then apply these concepts to produce simple command line applications. The concept of objects as entities containing data values and methods will be developed throughout the course. Students will utilize Java API class methods, and will also utilize instance methods for manipulating objects such as, Strings, arrays and ArrayLists. Both Scanner and JOptionPane object methods will be utilized for data input.
1	INFO-1120 Database Fundamentals		45	This course is an introduction to the design and development of database systems. Microsoft Access will be used to create a variety of simple databases. The database designs will be based upon typical requirements that a business may have with regards to their data

				management needs. Students will be responsible to build a complete database solution that incorporates the use of a multi-table database, forms, reports, queries and test data. Students will also be introduced to the Structured Query Language; SQL is the industry standard for querying databases.
1	INFO-1178 Configuring Windows Client		45	This course focusses on configuring and maintaining a Windows client operating system. Students learn to install and upgrade the operating system and manage drivers, applications, network connections, and resource access. Students learn how to create backups and use different recovery methods. The course can lead toward Microsoft certification.
1	PHIL-XXXX Ethics	X	45	This course provides an overview of the nature of ethics by examining a section of moral problems and ethical concerns that confront society today. Students will analyze and study ethical issues, concerns, and challenges in a business context. Theories will be applied to important ethical questions to gain an understanding of the issues behind them.
1 OR WRIT-1034 Reasoning & Writing 1 – EAP	WRIT-1043 Reasoning & Writing 1 for IT		45 OR 60	This course will introduce information technology students to essential principles of reading, writing, and reasoning at the postsecondary level. Students will identify, summarize, analyze, and evaluate multiple short readings and write persuasive response essays to develop their vocabulary, comprehension, grammar, and critical thinking. OR This course will introduce students whose first language is not English to essential principles of reading, writing, and reasoning at the postsecondary level. Students will identify, summarize, analyze, and evaluate multiple short readings and write persuasive response essays to develop their vocabulary, comprehension, grammar, and critical thinking. Special attention will also be paid to developing academic vocabulary, correcting common ESL errors, enhancing academic listening and note-taking skills, and improving oral fluency and confidence.
2	INFO-XXXX Network Components		60	This course will provide the students with a comprehensive overview of the concepts and operation of networking equipment in enterprise networks. The course will concentrate on the principles of switching and routing and the protocols involved. Topics will include Ethernet, STP, VLANs, 802.1q, IP protocol, and routing protocols. Switch and router security measures are employed throughout the course.

2	INFO-XXXX PHP Fundamentals		45	PHP is a widely-used open source general-purpose scripting language that is especially suited for web development. This course is designed to provide students with an overview of the PHP language, its main concepts, and the methodologies and best practices of coding professionally in PHP. Students will gain an understanding of the syntax and structural elements of PHP as well as accomplish tasks using PHP's array functions, understand essential elements of HTTP such as cookies and sessions, and interact with a database using PHP's MySQL functions
2	INFO-1124 Computer Security Concepts		45	Learn the basics for securing data on computer systems and the role of the ethical hacker and security professional. Topics in this course would demonstrate the security principles of Confidentiality, Integrity and Availability. Common hacker network attacks will be studied. Encryption methods used to secure data and authenticate users will be examined. Principles of password security and password cracking tools will be used in class.
2	INFO-XXXX Cryptography & Authentication Systems		45	Cryptography is a cornerstone of security technologies used to protect information and resources by providing secure communications. This course introduces students to modern cryptography with an emphasis on the fundamental cryptographic primitives of public key encryption, digital signatures, certificate and key management and basic protocols. Students will explore methods of protecting data by looking at how cryptography has evolved over the centuries to the complex methods of today. Students will also learn to recognize which encryption methods work best for given real-world situations.
2	INFO-XXXX Introduction to Unix		60	The UNIX operating system is a widely-used operating system underlying many of the services on the Internet. This course introduces students to the basics of the Unix operating system Students will learn the core utilities to work productively in a Linux environment and develop command line skills. Topics will include shell scripts and editing and managing files with an emphasis on the system-related security issues of these components.
2	CRIM-XXXX Cybercrime		45	This course introduces students to the legal and social issues related to cybercrime. Students will explore the origins of cybercrime, the evolution of threats, and the motivations and methods involved in cybercrime. Students will develop an understanding of the digital environment, hacker subculture, cyber stalking, and data

				theft.
2	INFO-XXXX Securing Windows Systems		45	Windows is still the most widely used operating system in business today, and, consequently, it is a major target to security attacks. In this course, students will acquire the knowledge and skills needed to configure, manage and secure the systems running on Microsoft Windows clients and servers. Students will investigate how Windows security technology works, how to assess vulnerabilities, and how to harden and monitor windows client and servers against attack. Active directory, group policies and PowerShell will also be explored as techniques to manage security.
3	COMM-3047 Communication for IT Professionals			This course provides students with the communication tools and skills typically used in an information technology workplace. Students develop skills in research, business writing, and technical writing. They conduct research, as well as analyze and organize information. Students gain skills with a variety of workplace documents, including e-mails, letters, manuals, informal and formal reports.
3	COOP-1020 Co-operative Education Employment Preparation			This workshop will provide an overview of the Co-operative Education consultants and students' roles and responsibilities as well as the Co-operative Education Policy. It will provide students with employment preparatory skills specifically related to co-operative education work assignments and will prepare students for their work term.
3	INFO-XXXX Security Management			The objective of Security Management is to ensure the confidentiality, integrity and availability of an organization's information, data and IT services. This course will concentrate on developing and implementing IT security strategies and methods. The necessary skills to identify and evaluate security management systems will also be provided. Students will prepare and determine how risk can be measured and managed.
3	INFO-XXXX Web Security			A website with weak security makes a network more vulnerable to attack and data loss more likely. This course covers how core web technologies work and includes the common security vulnerabilities of web sites today. Students will learn about the security threats, software vulnerabilities, and hacker attacks that are commonly implemented against commercial applications, including SQL injection, Cross-Site Scripting, and session hijacking. Students will also learn how to design and administer web services and applications using collaborative web tools and content management software.

3	INFO-XXXX Wireless and Mobile			Mobile phones and tablets have become essential to business, and the pervasive use of these devices has brought about new security risks. This course will examine the risks and vulnerabilities in the use of wireless and mobile networks. Students will implement and actively manage the security configuration of wireless and mobile devices in order to prevent attackers from exploiting vulnerable services and settings.
3	INFO-XXXX Network Protocols			Protocols are the backbone of networking and are formal sets of rules that dictate the ways in which computers communicate with one another over a network medium. This course will provide students with a detailed understanding of the protocols used in network communication. Students will explore the service definitions and analyze the protocols at each of the seven layers of both the OSI and TCP/IP models. The implications of adding security mechanisms to high-level network protocols operating in an open-system environment are analyzed.
3	INFO-XXXX Security Mechanisms			The course will examine security mechanisms including biometric technologies, smart card technologies, verification techniques, and cybersecurity protocols and review how they are used to help secure environments. Subjects to be reviewed include access control, identity and access control management and procedures, and exploration and analysis of biometric systems based on physiological and behavioral characteristics such as iris and retina patterns, fingerprinting, and facial features as well as systems based on behavioral characteristics such as graphology, keystroke dynamics, and gait. Students will also analyze how public institutions utilize biometrics and smartcards for cybersecurity systems for identification, authentication, and verification.
3	INFO-XXXX Digital Forensics			Digital forensics is the application of discovering and presenting evidence that has been obtained from computing and storage devices. Students will learn techniques to preserve and analyze digital evidence, and to reconstruct a timeline of events relevant to an incident. Students will employ professional digital forensic investigative procedures to ensure that evidence collected meets legal standards as it relates to both civil and criminal investigations.
4	Co-operative Education Placement			
5	INFO-XXXX Secure Scripting and Automation		45	To assist with common and repetitive tasks and to automate processes, system administrators often write

				and modify scripts. In this course, students will use a variety of tools and frameworks to write scripts that would handle system administration tasks such as managing files, services, or security controls. Students will also write scripts for test automation and batch processes.
5	INFO-XXXX LAMP Security		60	LAMP is an archetypal model of web service solution stacks of open-source components best used for building dynamic web sites and web applications. This course builds on the concepts and techniques of building PHP applications using relational databases as taught in PHP. Through both lectures and hands-on instruction, students will be introduced to advanced LAMP concepts and techniques used to build flexible and scalable web applications, build and deploy large web solutions, and secure them.
5	INFO-XXXX Network Monitoring and Change Management		60	This course will explore the components of a log collection system as well as log file management and optimization of the log review process through the correlation of events and real time alerts. Logs will be analyzed for such things as spotting patterns, incorrect information, and parsing logs. Security information and event management are also explored. Changes are a part of IT management and can have a substantial impact to an organization. Students will explore how to introduce and manage change in a controlled and coordinated manner.
5	INFO-XXXX Auditing and Security Controls		45	A primary security focus is the safeguards implemented to protect businesses and their assets, but it is imperative to determine if those protective measures are actually working. This course will concentrate on the concepts of auditing, controls and security in an IT environment. Topics covered include auditing, governance, internal controls, standards, guidelines and regulations. Methods and procedures to assess the risks and evaluate controls over information systems in an organization will be examined.
5	INFO-XXXX Evolving Technologies and Threats		45	The traditional network and how it is used is changing with the introduction of virtualization, Cloud computing, the Internet of Things, and SDN. This course will study how these technologies will impact the security and integrity of data. This course will also examine systems that are increasingly at risk such as mission critical systems (e.g., SCADA).
5	INFO-XXXX Computational Intelligence		45	Computational intelligence employs concepts, models, algorithms and tools such as Geographical Information

				Systems (GIS) and 3D modelling to map, track, analyze, and present digital evidence. This course will introduce the student to the fundamental principles of GIS, including what information is measureable using GIS; how this information, in the form of data, contributes to the knowledge, evidence, wisdom, and understanding of unethical activity; and how ranking data and information can present viable and evidence-based solutions to the complex social and technological problems of the 21st century.
5	CRIM-3001 Criminology	X	45	This course introduces students to the study of crime and delinquency within a Canadian context. Topics included for study are the making of laws, the elements of crime, crime statistics, correlates and theories of crime, specific forms of crime and strategies for crime law.
6	Co-operative Education Placement			
7	INFO-XXXX Perimeter Defense and Design		60	Modern security attacks today are far more advanced and require a multi-layered approach to ensure a network is secure. This course will investigate key concepts in the analysis of network traffic through deep packet inspection. Traditional perimeter defense systems such as firewalls, VPN's and Intrusion Prevention systems will be examined as well as the implementation of endpoint security systems.
7	INFO-XXXX Attack Vectors and Analysis		45	Attack vectors are the methods and techniques hackers use to exploit system vulnerabilities and gain access to a network for malicious intent. Students will analyze and investigate the various techniques hackers use to gain access to corporate data and bypass security measures. This course will examine a variety of real-life case studies that include study attack data and analysis of threats.
7	INFO-XXXX Penetration Testing		60	Penetration testing focuses on finding and analyzing vulnerabilities in a target environment. This course examines the legal issues involving ethical hacking to test corporate defense systems. The critical phases of an attack – scanning, enumeration, foot-printing, and social engineering – will be explored. Students will also be introduced to the latest ethical hacking tools and techniques to test corporate security systems.
7	INFO-XXXX Incidence Handling and Response		45	An increasing number of IT security threats can disrupt business activities and damage assets. Businesses need to have an incidence response mechanism or procedure capable of detecting and containing incidents, mitigating the impact of those incidents, and restoring services as

				quickly as possible. In this course, students will learn to design and manage key business information security functions including incident response, disaster recovery, and business continuity plans. Planning, reporting and budgeting are all addressed. Students will use business case studies to analyze and develop effective plans and solutions for various business scenarios.
7	INFO-XXXX Technical Writing and Presentation		45	In this course, students will learn how to use a systematic process for writing effective technical documents and creating presentations for the IT security professional. Emphasis will be on the written and spoken language using an analytical approach to critically assess and evaluate academic texts. Students will be expected to apply academic conventions and proper citation in the writing and presentation of appropriate documentation. Effective team building and communication in a culturally diverse and international environment will also be explored.
7	INFO-5096 Managing & Budgeting Technical Projects		45	Managing IT projects requires a multi-disciplinary approach that involves critical analysis, written and verbal communication skills, and interpersonal teambuilding skills. Creating and responding to RFPs, working with / as outsourced vendors, identifying tasks and resources required, budgets, timelines, and ongoing project maintenance are discussed. Students will use Microsoft Project and other tools to simulate resource scheduling, track progress, perform reporting, and close a project.
7	GEED-XXXX General Education Elective	X	45	
8	Co-operative Education Placement			
9	INFO-XXXX Research Project & Entrepreneurship		75	In this course, students will synthesize the theoretical and practical skills gained throughout the program in a research project that will address a specific cyber security issue. Case studies and/or live client scenarios will be presented, and students will have the opportunity to explore or develop security solutions to meet a company or organization's needs. Students will also be introduced to the fundamental concepts of entrepreneurship and examine the steps involved in developing and marketing their own IT security business or services.
9	INFO-XXXX Hacking Techniques and Exploits		60	In this course, students will examine the tools and techniques used to exploit vulnerabilities, the methods of attack, and how to defend against them. Examining the ways in which vulnerable systems can be attacked, will

				help students to identify means to better defend systems. The phases of ethical hacking, gaining access, maintaining access and covering one's tracks will be highlighted.
9	INFO-XXXX Advanced Penetration Testing		60	This course builds on the concepts of penetration testing. Students perform testing of typical security systems and web sites based on theories presented in other courses. Student will acquire in-depth knowledge of attack vectors. They will be provided with an environment in which to perform these attacks as part of numerous hands-on scenarios. The methodology of a given attack is discussed to find significant flaws in a target environment and demonstrate the business risk associated with these flaws.
9	INFO-XXXX Malware Analysis and Response		60	Malware analysis is the study of malware by dissecting their different components and studying their behavior to better assess the nature of the security incident and help prevent future attacks. This course will examine the behaviour of a program to provide deeper insight into attacker tools and tactics and key characteristics of malware present on compromised systems. Concepts of reverse engineering and behavioural and code analysis will be used to analyze the malware attack lifecycle from the initial exploit.
9	INFO-XXXX Secure Network Architecture		45	In this course, students will incorporate all of the security solutions they have learned over the course of the program to develop and deploy security architecture components that allow for scalable and secure IT infrastructures. This course will combine planning policies with offensive and defensive techniques to defend a network from all threats.
9	GEED-XXXX General Education Elective	X	45	

Add additional rows as required to complete the curriculum chart.

I. REGULATORY STATUS FORM (APPENDIX D)

Please complete the following:

There IS a legislative requirement that program graduates must be certified or licensed by a regulatory authority to practice or work in the occupation

☐ **Mandatory recognition of a regulatory authority exists and is being sought.**
(Please refer to Section A below- *Mandatory Regulatory Requirements*)

There IS or IS NOT a voluntary (i.e., not required by legislation) licensing or certification for entry to practice in the profession or trade.

☐ YES
☒ NO

☐ **Voluntary recognition of a regulatory authority IS being sought.**
(Please refer to Section B below- *Recognition by Voluntary Association*)

☐ **Voluntary recognition is NOT being sought***.
Please explain why: Click here to enter text.

*Note: *There may be titling implications for programs that are not seeking recognition in an area where existing programs have secured recognition.*

A. MANDATORY REGULATORY REQUIREMENTS

Where licensing or certification is ***required by legislation*** for entry to practice in the profession or trade, the Ministry of Training, Colleges and Universities requires that colleges ensure that their programs will meet the requirements of the regulatory body in order to be approved for funding.

Name of regulatory authority:

Status (please select ALL that apply)

☐ Accreditation or approval by the regulatory authority / designated third party received.
Date of recognition:

☐ The college is working toward accreditation with the regulatory authority/ designated third party.
Describe current status of application:
Expected date of recognition:

☐ The regulatory authority does not accredit educational programs directly or through designated third party. Formal acknowledgement (e.g. in its published or legislated registration requirements) that the program graduates will be eligible to write any required certifying or registration exam(s) or that the program is otherwise recognized for the purposes of certifying or registering a graduate is being sought.

Please submit an acknowledgement and/or evidence from the regulatory authority regarding the status of the recognition.

B. RECOGNITION BY VOLUNTARY ASSOCIATION

Colleges may choose to have a program accredited or recognized by a voluntary membership organization or association. Graduate eligibility for association recognition or adherence to standards imposed by the body is ***a recommendation and not a requirement*** for program funding approval by the Ministry of Training, Colleges and Universities.

Name of voluntary association:

Status (please select ALL that apply)

☐ The college is working toward recognition.
Describe current status of application:
Expected date of recognition:

☐ Recognition has been received.
Date of recognition:
Type of recognition (e.g. accreditation, graduates eligible to write membership exams, etc.):

☐ The association does not recognize educational programs directly or through designated third party. Formal recognition (e.g. in its published requirements) that the program graduates will be eligible to write any required certifying or registration exam(s) or that the program is otherwise recognized for the purposes of certifying or registering a graduate is being sought.

Please submit an acknowledgement and/or evidence from the regulatory authority or voluntary association regarding the status of the recognition.

APPENDIX E – Program Outcomes – Curriculum Map

PROGRAM MAPPING Cyber Security														
	LEVEL ONE							**LEVEL TWO**						
PROGRAM VOCATIONAL LEARNING OUTCOMES														
1 - Introductory **2** - Building **3** - Culminating **The graduate has reliably demonstrated the ability to: (Source: MTCU Code)**	INFO-1135 Networking Fundamentals	INFO-1150 Programming Fundamentals	INFO-1120 Database fundamentals	INFO-1178 Configuring Windos Client	PHIL-XXXX Ethics (GM)	WRIT-1043 Reasoning & Writing for IT/ WRIT-1034 Reasoning & Writing - EAP		INFO-XXXX Network Components	INFO-XXXX PHP Fundamentals	INFO-1124 Security Concepts	INFO-XXXX Cryptography and Authentication Systems	INFO-XXXX Introduction to Unix	CRIM-XXXX - Cybercrime	INFO-XXXX Securing Windows Systems	**# OF COURSES EVALUATING THE OUTCOME**
1. Configure, implement, manage and secure devices and equipment considering the unique features of the computer operating systems, networks, applications and software.	**1**	**1**	**1**	**1**				**2**	**1**	**1**	**2**	**1**		**1**	**10**
2. Design, implement and evaluate security solutions for business processes, applications and communications to protect business resources and respond to the needs of all the internal stakeholders.	**1**	**1**	**1**	**1**				**2**	**1**	**1**	**2**	**1**		**1**	**10**
3. Use project management principles to implement security strategies and processes that address the organization's information security requirements.										**1**					**1**
4. Develop, implement and evaluate organizational security policies, standards and regulations to promote internal security.	**1**	**1**	**1**	**1**				**2**	**1**	**1**	**1**	**1**		**1**	**10**
5. Perform vulnerability assessments and penetration testing for infrastructures, web and applications, using both manual and automated techniques.		**1**								**1**				**1**	**3**
6. Evaluate and apply tools and techniques to formulate countermeasures to secure information systems against security threats.	**1**	**1**	**1**	**1**				**2**	**1**	**1**	**2**			**1**	**9**
7. Perform security audits and forensic analysis to evaluate the effectiveness of a security system, and identify and correct security vulnerabilities.													**1**		**1**
8. Monitor and analyze logs and alerts from network devices to determine the extent of a security breach and what data has been compromised.	**1**							**2**	**1**						**3**
9. Identify, collect, and log relevant data as evidence for a sample case within a business or in the Canadian Justice System.					**1**					**1**			**1**		**3**
TOTAL # OF OUTCOMES EVALUATED BY EACH COURSE	**5**	**5**	**4**	**4**	**1**	**0**		**5**	**5**	**7**	**4**	**3**	**2**	**5**	
GM = General Education (mandatory) G = General Education (elective)															

NB - Only indicate the outcomes that are Taught & Evaluated (TE or TRE) in a course

PROGRAM COORDINATOR: TBD

ACADEMIC CHAIR: Jim Edwards

Date Completed: October 2015

Analysis of Mapping Results:

PROGRAM MAPPING (Name of Program)																	
	LEVEL THREE									LEVEL FOUR							
PROGRAM VOCATIONAL LEARNING OUTCOMES **1** - Introductory **2** - Intermediate **3** - Advanced **The graduate has reliably demonstrated the ability to: (Source: MTCU Code)**	COMM-3047 Communication for IT Professionals	COOP-1020 Co-operative Education Employment Prep	INFO-XXXX Security Management	INFO-XXXX Web Security	INFO-XXXX Wireless and Mobile Devices	INFO-XXXX Security Mechanisms	INFO-XXXX Digital Forensics	INFO-XXXX Network Protocols		INFO-XXXX Scripting and Automation	INFO-XXXX LAMP Security	INFO-XXXX Network Monitoring and Change Management	INFO-XXXX Auditing and Security Controls	CRIM-3001 Criminology (GM)	INFO-XXXX Evolving Technologies and Threats	INFO-XXXX Computational Intelligence	**# OF COURSES EVALUATING THE OUTCOME**
1. Configure, implement, manage and secure devices and equipment considering the unique features of the computer operating systems, networks, applications and software.				2	2	2	1	3		2	2	2			2	2	10
2. Design, implement and evaluate security solutions for business processes, applications and communications to protect business resources and respond to the needs of all the internal stakeholders.			1	2	2	2		3		2	2	2	2		2		10
3. Use project management principles to implement security strategies and processes that address the organization's information security requirements.			1									2	2				3
4. Develop, implement and evaluate organizational security policies, standards and regulations to promote internal security.			1	2	2	2	1	2		2	2	2	2		2	2	12
5. Perform vulnerability assessments and penetration testing for infrastructures, web and applications, using both manual and automated techniques.			1									2	2				3
6. Evaluate and apply tools and techniques to formulate countermeasures to secure information systems against security threats.			1	2	2	2	1	3		2	2	2	2		2	2	12
7. Perform security audits and forensic analysis to evaluate the effectiveness of a security system, and identify and correct security vulnerabilities.			1			1	1					2	2				5
8. Monitor and analyze logs and alerts from network devices to determine the extent of a security breach and what data has been compromised.			1		2	2	2	3		2	2	2	2				9
9. Identify, collect, and log relevant data as evidence for a sample case within a business or in the Canadian Justice System.						1	2					1	2	3		3	6
TOTAL # OF OUTCOMES EVALUATED BY EACH COURSE	0	0	7	4	5	7	6	5		5	5	9	8	1	4	4	
V = Vocational Courses E = Essential Employability Skills Courses																	
GM = General Education (mandatory) G = General Education (elective)																	

NB - Only indicate the outcomes that are Taught & Evaluated (TE or TRE) in a course

PROGRAM COORDINATOR: TBD

ACADEMIC CHAIR: Jim Edwards

Date Completed: October 2015

Analysis of Mapping Results:

PROGRAM MAPPING (Name of Program)																
	LEVEL FIVE								LEVEL SIX							
PROGRAM VOCATIONAL LEARNING OUTCOMES **1** - Introductory **2** - Intermediate **3** - Advanced **The graduate has reliably demonstrated the ability to: (Source: MTCU Code)**	INFO-XXXX Perimeter Defense and Design	INFO-XXXX Attack Vectors and Analysis	INFO-XXXX Penetration Testing	INFO-XXXX Incidence Handling and Response	INFO-5096 Managing & Budgeting Technical Projects	INFO-XXXX Technical Writing and Presentations	GEED-XXXX General Education Elective (G)		GEED-XXXX General Education Elective (G)	INFO-XXXX Research Project & Entrepreneurship	INFO-XXXX Hacking Techniques and Exploits	INFO-XXXX Advanced Penetration Testing	INFO-XXXX Malware Analysis and Response	INFO-XXXX Secure Network Architecture	**# OF COURSES EVALUATING THE OUTCOME**	**TOTAL FOR PROGRAM**
1. Configure, implement, manage and secure devices and equipment considering the unique features of the computer operating systems, networks, applications and software.	**3**	**3**	**3**	**3**		**3**				**2**	**3**	**3**		**3**	**9**	**29**
2. Design, implement and evaluate security solutions for business processes, applications and communications to protect business resources and respond to the needs of all the internal stakeholders.	**3**	**3**	**3**	**3**	**2**	**3**				**3**			**3**	**3**	**9**	**29**
3. Use project management principles to implement security strategies and processes that address the organization's information security requirements.					**3**	**3**				**3**					**3**	**7**
4. Develop, implement and evaluate organizational security policies, standards and regulations to promote internal security.	**3**	**3**	**3**	**3**		**3**				**2**				**3**	**7**	**29**
5. Perform vulnerability assessments and penetration testing for infrastructures, web and applications, using both manual and automated techniques.	**3**	**3**	**3**	**3**		**3**				**2**	**3**	**3**			**8**	**14**
6. Evaluate and apply tools and techniques to formulate countermeasures to secure information systems against security threats.	**3**	**3**	**3**	**3**		**3**				**3**	**3**	**3**			**8**	**29**
7. Perform security audits and forensic analysis to evaluate the effectiveness of a security system, and identify and correct security vulnerabilities.	**3**	**3**	**3**	**3**		**3**				**3**					**6**	**12**
8. Monitor and analyze logs and alerts from network devices to determine the extent of a security breach and what data has been compromised.	**3**	**3**	**3**	**3**		**3**				**2**				**3**	**7**	**19**
9. Identify, collect, and log relevant data as evidence for a sample case within a business or in the Canadian Justice System.		**2**				**1**				**2**	**2**				**4**	**13**
TOTAL # OF OUTCOMES EVALUATED BY EACH COURSE	**7**	**8**	**7**	**7**	**2**	**9**	**0**		**0**	**9**	**4**	**3**	**1**	**4**		
V = Vocational Courses E = Essential Employability Skills Courses **GM = General Education (mandatory) G = General Education (elective)**																

NB - Only indicate the outcomes that are Taught & Evaluated (TE or TRE) in a course

PROGRAM COORDINATOR: TBD

ACADEMIC CHAIR: Jim Edwards

Date Completed: October 2015

Analysis of Mapping Results:

APPENDIX E – Program Outcomes – Curriculum Map

PROGRAM MAPPING Cyber Security															
	LEVEL ONE							**LEVEL TWO**							
PROGRAM ESSENTIAL EMPLOYABILITY SKILLS OUTCOMES **4 = R 5 = RE 6 = TE 7 = TRE**	INFO-1135 Networking Fundamentals	INFO-1150 Programming Fundamentals	INFO-1120 Database fundamentals	INFO-1178 Configuring Windos Client	PHIL-XXXX Ethics (GM)	WRIT-1043 Reasoning & Writing for IT/ WRIT-1034 Reasoning & Writing - EAP		INFO-XXXX Network Components	INFO-XXXX PHP Fundamentals	INFO-1124 Security Concepts	INFO-XXXX Cryptography and Authentication Systems	INFO-XXXX Introduction to Unix	CRIM-XXXX - Cybercrime	INFO-XXXX Securing Windows Systems	**# OF COURSES SUPPORTING THE OUTCOME**
1. communicate clearly, concisely and correctly in the written, spoken, and visual form that fulfills the purpose and meets the needs of the audience.	**4**	**6**	**5**	**4**	**6**	**6**		**5**	**6**	**5**	**5**	**5**	**5**	**4**	**13**
2. respond to written, spoken, or visual messages in a manner that ensures effective communication.	**5**			**5**	**6**	**6**		**4**		**5**	**4**	**5**	**4**	**5**	**10**
3. execute mathematical operations accurately.	**4**	**6**	**5**	**7**				**7**	**6**		**7**	**4**	**4**	**7**	**10**
4. apply a systematic approach to solve problems.	**7**	**6**	**7**	**7**		**6**		**7**	**6**		**7**	**7**	**7**	**7**	**11**
5. use a variety of thinking skills to anticipate and solve problems.	**7**	**4**	**7**	**7**		**6**		**7**	**4**		**7**	**5**	**7**	**7**	**11**
6. locate, select, organize, and document information using appropriate technology and information systems.	**6**	**6**	**7**	**6**	**6**	**6**		**7**	**6**		**6**	**5**	**7**	**6**	**12**
7. analyze, evaluate, and apply relevant information from a variety of sources.	**6**	**4**	**5**	**5**	**6**	**6**		**4**	**4**		**6**	**5**	**6**	**5**	**12**
8. show respect for the diverse opinions, values, belief systems, and contributions of others.	**5**	**4**	**5**	**4**	**7**	**4**		**4**	**4**		**4**	**4**	**4**	**4**	**12**
9. interact with others in groups or teams in ways that contribute to effective working relationships and the achievement of goals.	**4**	**4**	**5**			**4**		**4**	**4**	**4**	**4**	**4**	**4**		**10**
10. manage the use of time and other resources to complete projects.	**7**	**4**	**5**	**5**		**4**		**7**	**4**	**5**	**6**	**5**	**6**	**5**	**12**
11. take responsibility for one's own actions, decisions, and consequences.	**6**	**4**	**5**	**5**	**7**	**4**		**4**	**4**		**4**	**5**	**4**	**5**	**12**
TOTAL # OF OUTCOMES SUPPORTED BY EACH COURSE	**11**	**10**	**10**	**10**	**6**	**10**		**11**	**10**	**4**	**11**	**11**	**11**	**10**	

PROGRAM COORDINATOR: TBD

ACADEMIC CHAIR: Jim Edwards

Date Completed: October 2015

Analysis of Mapping Results:

PROGRAM MAPPING (Name of Program)																
	LEVEL THREE									LEVEL FOUR						
PROGRAM ESSENTIAL EMPLOYABILITY SKILLS OUTCOMES **4 = R 5 = RE 6 = TE 7 = TRE** **T = Taught R = Reinforced E = Evaluated** **The graduate has reliably demonstrated the ability to: (Source: MTCU Code)**	COMM-3047 Communication for IT Professionals	COOP-1020 Co-operative Education Employment Prep	INFO-XXXX Security Management	INFO-XXXX Web Security	INFO-XXXX Wireless and Mobile Devices	INFO-XXXX Security Mechanisms	INFO-XXXX Digital Forensics	INFO-XXXX Network Protocols		INFO-XXXX Scripting and Automation	INFO-XXXX LAMP Security	INFO-XXXX Network Monitoring and Change Management	INFO-XXXX Auditing and Security Controls	CRIM-3001 Criminology (GM)	INFO-XXXX Evolving Technologies and Threats	INFO-XXXX Computational Intelligence	**# OF COURSES SUPPORTING THE OUTCOME**
1. communicate clearly, concisely and correctly in the written, spoken, and visual form that fulfills the purpose and meets the needs of the audience.	7	4	4	4	4	4	4	4		6	4	5	4	5	4	4	15
2. respond to written, spoken, or visual messages in a manner that ensures effective communication.	7	4	5	5	4	4	4	4			5	4	5	5	5	5	14
3. execute mathematical operations accurately.			4	4				6		6	4	7	4		4	5	9
4. apply a systematic approach to solve problems.	7		7	7		5	6	5		6	7	7	7	4	5	6	13
5. use a variety of thinking skills to anticipate and solve problems.	4		7	7	7	4	6	4		4	7	7	7	7	5	6	14
6. locate, select, organize, and document information using appropriate technology and information systems.	7	5	6	6	7		7	4		6	6	7	6	7	5	6	14
7. analyze, evaluate, and apply relevant information from a variety of sources.	7	5	6	6	7		7	4		4	6	4	6	7	5	6	14
8. show respect for the diverse opinions, values, belief systems, and contributions of others.	4	4	5	5	4		4	4		4	5	4	5	5		4	13
9. interact with others in groups or teams in ways that contribute to effective working relationships and the achievement of goals.	7	4	4	4	4	4	4	4		4	4	4	4	7		4	14
10. manage the use of time and other resources to complete projects.	7	4	7	7	4	5	4	5		4	7	7	7	4		6	14
11. take responsibility for one's own actions, decisions, and consequences.	4	4	6	6	4	4	4	4		4	6	4	6	4		6	14
TOTAL # OF OUTCOMES SUPPORTED BY EACH COURSE	10	8	11	11	9	7	10	11		10	11	11	11	10	7	11	

PROGRAM COORDINATOR: TBD

ACADEMIC CHAIR: Jim Edwards

Date Completed: October 2015

Analysis of Mapping Results:

PROGRAM MAPPING (Name of Program)																
	LEVEL FIVE								LEVEL SIX							
PROGRAM ESSENTIAL EMPLOYABILITY SKILLS OUTCOMES **4 = R 5 = RE 6 = TE 7 = TRE** **T = Taught R = Reinforced E = Evaluated** **The graduate has reliably demonstrated the ability to: (Source: MTCU Code)**	INFO-XXXX Perimeter Defense and Design	INFO-XXXX Attack Vectors and Analysis	INFO-XXXX Penetration Testing	INFO-XXXX Incidence Handling and Response	INFO-5096 Managing & Budgeting Technical Projects	INFO-XXXX Technical Writing and Presentations	GEED-XXXX General Education Elective (G)		GEED-XXXX General Education Elective (G)	INFO-XXXX Research Project & Entrepreneurship	INFO-XXXX Hacking Techniques and Exploits	INFO-XXXX Advanced Penetration Testing	INFO-XXXX Malware Analysis and Response	INFO-XXXX Secure Network Architecture	**# OF COURSES SUPPORTING THE OUTCOME**	**TOTAL FOR PROGRAM**
1. communicate clearly, concisely and correctly in the written, spoken, and visual form that fulfills the purpose and meets the needs of the audience.	4	4	4	4	4	6				6	4	4	4	4	11	39
2. respond to written, spoken, or visual messages in a manner that ensures effective communication.	5	5	5	5	5	6				6	5	5	5	5	11	35
3. execute mathematical operations accurately.	4	4	4	4	7					4	4	4	4	4	10	29
4. apply a systematic approach to solve problems.	7	7	7	7	6	4				7	7	7	7	7	11	35
5. use a variety of thinking skills to anticipate and solve problems.	7	7	7	7	5	4				7	7	7	7	7	11	36
6. locate, select, organize, and document information using appropriate technology and information systems.	6	6	6	6	5	6				7	6	6	6	6	11	37
7. analyze, evaluate, and apply relevant information from a variety of sources.	6	6	6	6	5	6				7	6	6	6	6	11	37
8. show respect for the diverse opinions, values, belief systems, and contributions of others.	5	5	5	5	6	6				4	5	5	5	5	11	36
9. interact with others in groups or teams in ways that contribute to effective working relationships and the achievement of goals.	4	4	4	4	6	4				4	4	4	4	4	11	35
10. manage the use of time and other resources to complete projects.	7	7	7	7	7	4				6	7	7	7	7	11	37
11. take responsibility for one's own actions, decisions, and consequences.	6	6	6	6	6	5				4	6	6	6	6	11	37
TOTAL # OF OUTCOMES SUPPORTED BY EACH COURSE	11	11	11	11	11	10	0		0	11	11	11	11	11		

PROGRAM COORDINATOR: TBD

ACADEMIC CHAIR: Jim Edwards

Date Completed: October 2015

Analysis of Mapping Results:

APPENDIX F

Program Delivery Information (PDI) Form to Calculate Program Funding Parameters
Total Hours Required per Student

College: Fanshawe College Program title: Cyber Security

Indicate the number of hours that a student is required to spend in each instructional setting in each semester or level of this program. All hours in all instructional settings are to be noted.

Funded Instructional Settings*	**Semester/Level**									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Total**
Classroom instruction	**210**	**195**	**186**		**195**		**225**		**120**	**1131**
Laboratory/workshop/ fieldwork	**120**	**135**	**150**		**150**		**120**		**225**	**900**
Independent (self-paced) learning										
One-on-one instruction										
Clinical placement										
Field placement/work placement										
Small group tutorial										
TOTAL	**330**	**330**	**336**		**345**		**345**		**345**	**2031**

Non-funded Instructional Settings*	**Semester/Level**									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Total**
Co-op work placement - Mandatory				**300**		**300**		**300**		**900**
Co-op work placement - Optional										
TOTAL				**300**		**300**		**300**		**900**

*Definitions for each instructional setting can be found below.

Appendix G: Detailed Course Delivery

Program: Cyber Security **Term: Fall**
School: School of Information Security **Starting Year: 2017**

Course Code	Course Name	Hours	Weeks / Term	Course Status	No. of Sections	Proposed Section Size	Course Delivery Space (hours distribution per week)						Additional Comments
							Classroom	Laboratory	Dedicated Space	Computer Room	Other (describe)	None	
Level 1													
INFO-1135	Networking Fundamentals	75	15	Existing	1	30			5				Networking/Security lab
INFO-1150	Programming Fundamentals	75	15	Existing	1	30	5						
INFO-1120	Datbase Fundamentals	45	15	Existing	1	30	3						
INFO-1178	Configuring Windows Client	45	15	Existing	1	30			3				Networking/Security lab
PHIL-XXXX	Ethics	45	15	New	1	30	3						
WRIT-1043	Reasoning & Writing 1 for IT	45	15	Existing	1	30	3						
or WRIT-1034	Reasoning & Writing 1 - EAP	60	15	Existing	1	30	4						
	Total:	330	or 345										
Level 2													
INFO-XXXX	Network Components	60	15	New	1	30			4				Networking lab
INFO-XXXX	PHP Fundamentals	45	15	New	1	30	3						
INFO-1124	Computer Security Concepts	45	15	Existing	1	30			3				Networking/Security lab
INFO-XXXX	Cryptography & Authentication Systems	45	15	New	1	30			3				Networking/Security lab
INFO-XXXX	Introduction to UNIX	45	15	New	1	30	3						
CRIM-XXXX	Cyber Crime	45	15	New	1	30	3						
INFO-XXXX	Securing Windows Systems	45	15	New	1	30			3				
	Total:	330											
Level 3													
COMM-3047	Communication for IT Professionals	45	15	Existing	1	30	3						
COOP-1020	Co-operative Education Employment Prep	6	15	Existing	1	30	6						
INFO-XXXX	Security Management	45	15	New	1	30	3						
INFO-XXXX	Web Security	45	15	New	1	30	3						
INFO-XXXX	Wireless and Mobile	45	15	New	1	30			3				Networking/Security lab
INFO-XXXX	Network Protocols	60	15	New	1	30			4				Networking/Security lab
INFO-XXXX	Security Mechanisms	45	15	New	1	30			3				Networking/Security lab
INFO-XXXX	Digital Forensics	45	15	New	1	30	3						
	Total:	336											
Level 4													
	Co-op Placement												
Level 5													
INFO-XXXX	Secure Scripting and Automation	45	15	New	1	30	3						
INFO-XXXX	LAMP Security	60	15	New	1	30	4						
INFO-XXXX	Network Monitoring and Change Management	60	15	New	1	30			4				Networking lab
INFO-XXXX	Auditing and Security Controls	45	15	New	1	30	3						
INFO-XXXX	Evolving Technologies and Threats	45	15	New	1	30			3				Networking/Security lab
INFO-XXXX	Computational Intelligence	45	15	New	1	30			3				Networking/Security lab
CRIM-3001	Criminology	45	15	Existing	1	30	3						
	Total:	345											
Level 6													
	Co-op Placement												
Level 7													
INFO-XXXX	Perimeter Defense and Design	60	15	New	1	30			4				Networking/Security lab
INFO-XXXX	Attack Vectors and Analysis	45	15	New	1	30	3						
INFO-XXXX	Penetration Testing	60	15	New	1	30			4				Networking/Security lab
INFO-XXXX	Incidence Handling and Response	45	15	New	1	30	3						
INFO-XXXX	Technical Writing and Presentation	45	15	New	1	30	3						
GEED-XXXX	Gen Ed - Elective	45	15	New	1	30	3						
INFO-5096	Managing & Budgeting Technical Projects	45	15	New	1	30	3						
	Total:	345											
Level 8													
	Co-op Placement												
Level 9													
INFO-XXXX	Research Project and Entrepreneurship	75	15	New	1	30	5						
INFO-XXXX	Hacking Techniques and Exploits	60	15	New	1	30			4				Networking/Security lab
GEED-XXXX	Gen Ed - Elective	45	15	New	1	30	3						
INFO-XXXX	Advanced Penetration Testing	60	15	New	1	30			4				Networking/Security lab
INFO-XXXX	Secure Network Architecture	45	15	New	1	30			3				Networking/Security lab
INFO-XXXX	Malware Analysis and Response	60	15	New	1	30			4				Networking/Security lab
	Total:	345											

TOTAL: 2031 or 2046

APPENDIX H - Multi Year Budget with Proforma Analysis and Net Present Value Rating

Program Name CyberSecurity
Program type Advanced Diploma

		Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10	Total
Incremental revenues												
Grants:	Notes											
- program name	1	n/a	310,000	620,000	825,000	1,052,500	1,052,500	1,052,500	1,052,500	1,052,500	1,052,500	8,070,000
Tuition:												
- program name	2,3,4	258,032	516,064	678,923	872,770	872,770	872,770	872,770	872,770	872,770	872,770	7,562,411
Program Specific fee **	5	6,900	13,800	18,300	23,400	23,400	23,400	23,400	23,400	23,400	23,400	202,800
Other associated revenue		0	0	0	0	0	0	0	0	0	0	0
sub-total		264,932	839,864	1,317,223	1,721,170	1,948,670	1,948,670	1,948,670	1,948,670	1,948,670	1,948,670	15,835,211
Incremental expenses												
Indirect salaries:												
Admin/Support staff		0	0	0	0	0	0	0	0	0	0	0
Teaching salaries:												
Full time - number required		2	2	2	2	2	2	2	2	2	2	
- cost @	$129,061	258,122	258,122	258,122	258,122	258,122	258,122	258,122	258,122	258,122	258,122	2,581,220
Part time - hours per week req'd		16	106	152	196	196	196	196	196	196	196	
- cost @	see below	19,958	132,224	189,605	244,490	244,490	244,490	244,490	244,490	244,490	244,490	2,053,220
One time costs - facilities		0										0
fitup/equipment		0										0
Other startup		132,000										132,000
Operating expenses		0										0
Capital expenses		440,000		440,000		150,000			150,000			1,180,000
sub-total		850,080	390,346	887,727	502,612	652,612	502,612	502,612	652,612	502,612	502,612	5,946,440
incremental cash inflows		-585,149	449,517	429,496	1,218,558	1,296,058	1,446,058	1,446,058	1,296,058	1,446,058	1,446,058	9,888,770
	CTO%		54%	33%	71%	67%	74%	74%	67%	74%	74%	

Net present value @ 8% $5,810,720

Notes:
1. Grant based on existing ISN program
2. Tuition based on existing CTY/CPA program
3. 90%/10% domestic/international enrolments assumed
4. Based on lvl 1 enrolment total of 72 (for 2 intakes)

INPUT FIELDS

Tuition - domestic (per term)	lvl 1/2		$1,383.16
	lvl 3/4		$1,383.16
Grant (per term)	all levels		$2,500.00
Program specific fee	all levels		$50.00
Tuition - international (per term)	lvl 1/2		$6,180.00
	lvl 3/4		$6,180.00
Enrolment split	domestic		90%
	international		10%
Part time / Partial load	split %	PT	40%
		PL	60%
	hrly rate	PT	$51.15
	(incl. ben's)	PL	$104.50
Number of weeks for PT/PL			15

YEAR 1

Enrolment table

Program name			
	Domestic	Int'l	
Fall total	32	4	36
Winter total	62	7	69
Summer total	30	3	33
	0	0	
	124	14	138

Tuition rates

	Domestic	Int'l
level 1	1,383.16	6,180.00
level 2	1,383.16	6,180.00
level 3	1,383.16	6,180.00
level 4	1,383.16	6,180.00

Grant values

	Domestic	Int'l
level 1	2,500.00	0.00
level 2	2,500.00	0.00
level 3	2,500.00	0.00
level 4	2,500.00	0.00

YEAR 2

Enrolment table	Program name		
	Domestic	Int'l	
Fall total	92	10	102
Winter total	69	8	77
Summer total	87	10	97
	0	0	
	248	28	276

Tuition rates

	Domestic	Int'l
level 1	1,383.16	6,180.00
level 2	1,383.16	6,180.00
level 3	1,383.16	6,180.00
level 4	1,383.16	6,180.00

Grant values

	Domestic	Int'l
level 1	2,500.00	0.00
level 2	2,500.00	0.00
level 3	2,500.00	0.00
level 4	2,500.00	0.00

YEAR 3

Enrolment table	Program name		
	Domestic	Int'l	
Fall total	102	11	113
Winter total	131	14	145
Summer total	97	11	108
	0	0	0
	330	36	366

Tuition rates

	Domestic	Int'l
level 1	1,383.16	6,180.00
level 2	1,383.16	6,180.00
level 3	1,383.16	6,180.00
level 4	1,383.16	6,180.00

Grant values

	Domestic	Int'l
level 1	2,500.00	0.00
level 2	2,500.00	0.00
level 3	2,500.00	0.00
level 4	2,500.00	0.00

YEAR 4

Enrolment table	Program name		
	Domestic	Int'l	
Fall total	169	19	188
Winter total	144	16	160
Summer total	108	12	120
	0	0	0
	421	47	468

Tuition rates

	Domestic	Int'l
level 1	1,383.16	6,180.00
level 2	1,383.16	6,180.00
level 3	1,383.16	6,180.00
level 4	1,383.16	6,180.00

Grant values

	Domestic	Int'l
level 1	2,500.00	0.00
level 2	2,500.00	0.00
level 3	2,500.00	0.00
level 4	2,500.00	0.00

Appendix I: Student Demand

As of August 26, 2015

Student Demand -MTCU 63002 Information Security Technology - L'INFORMATION

	APPLICATIONS				ENROLMENT				INT - ENROLMENT			
	2011	2012	2013	2014	2011	2012	2013	2014	2011	2012	2013	2014
FLEMING	89	80	78	84	36	34	29	25	0	0	1	1
LA CITÉ COLLÉGIALE	55	55	8	0	21	0	0	0	0	0	0	0
	144	135	86	84	57	34	29	25	0	0	1	1

WHERE IS FANS CATCHMENT GOING?

	APPLICATIONS				ENROLMENT			
	2011	2012	2013	2014	2011	2012	2013	2014
FLEMING	0	2	3	2	0	2	0	0
LA CITÉ COLLÉGIALE	0	1	0	0	0	0	0	0
	0	3	3	2	0	2	0	0

Note: The program offered at La Cité Collégiale was suspended for a few years and is now being offered in Fall 2015.

Appendix J: Labour Market Demand

Information Systems Analysts and Consultants (NOC-S C071)

For the London CMA, the Information Systems Analysts and Consultants (NOC-S C071) occupation shows an increase in the number of jobs by 176 for the 2014-2021 period or 25 additional jobs per year. All of the neighboring London CMA regions show projected job growth. The shift share analysis shows that 50% of the projected job change for London CMA could be attributed to its competitive advantage. Given this advantage, it is not strange to see that the concentration of this type of jobs in London is growing (see location quotient analysis).

The province shows similar growth in employment. It is projected an increase of 4389 or 627 jobs per year for the period 2014-2021.

For information systems analyst and consultants, opportunities will be raising from the expansion of e-health technologies, the demand for computer security and cloud computing[1].

2171-Information Systems Analysts and Consultants (NOC-S C071)

1. Projected New Jobs

Projected jobs represents newly created positions. These projections do not account for new replacement jobs due to attrition or any anomalies such as hiring freezes, early leavers, etc.

Change and % Change represent the difference in the number or percentage of jobs for the entire period of analysis.

[1] Job Bank Canada. Outlook report. Source: http://www.jobbank.gc.ca/LMI_report_bynoc.do?&noc=2171&reportOption=outlook Last update: May 29, 2015

Figure 1. Actual and projected percentage jobs from 2014 to 2021 for London CMA, Ontario, and Canada

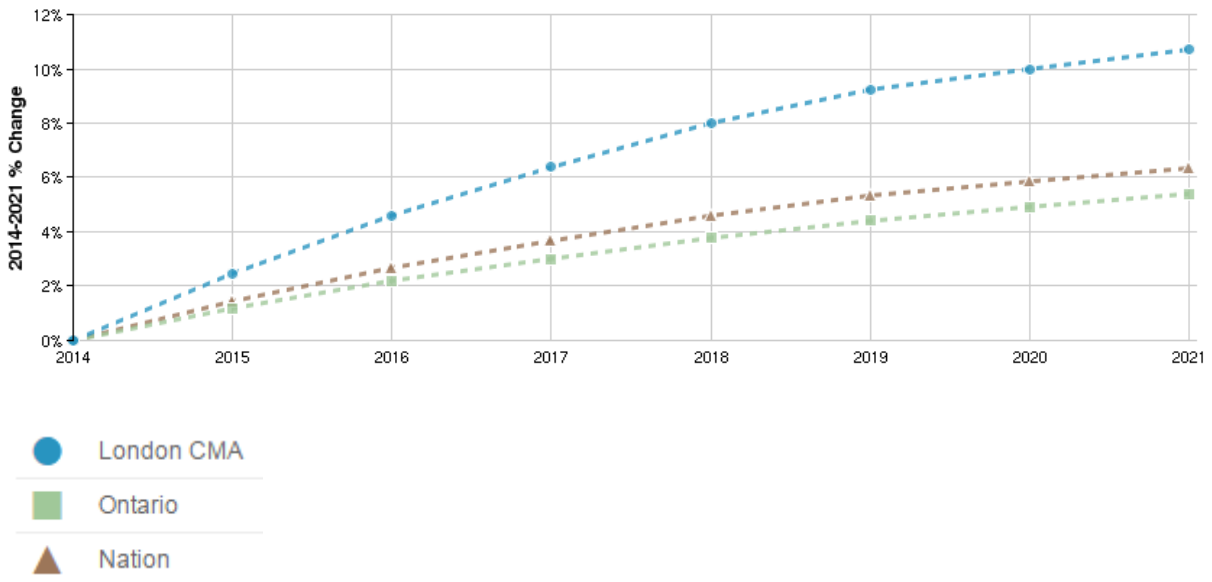


Table 1. Net projected regional percentage job change (2014-2021)

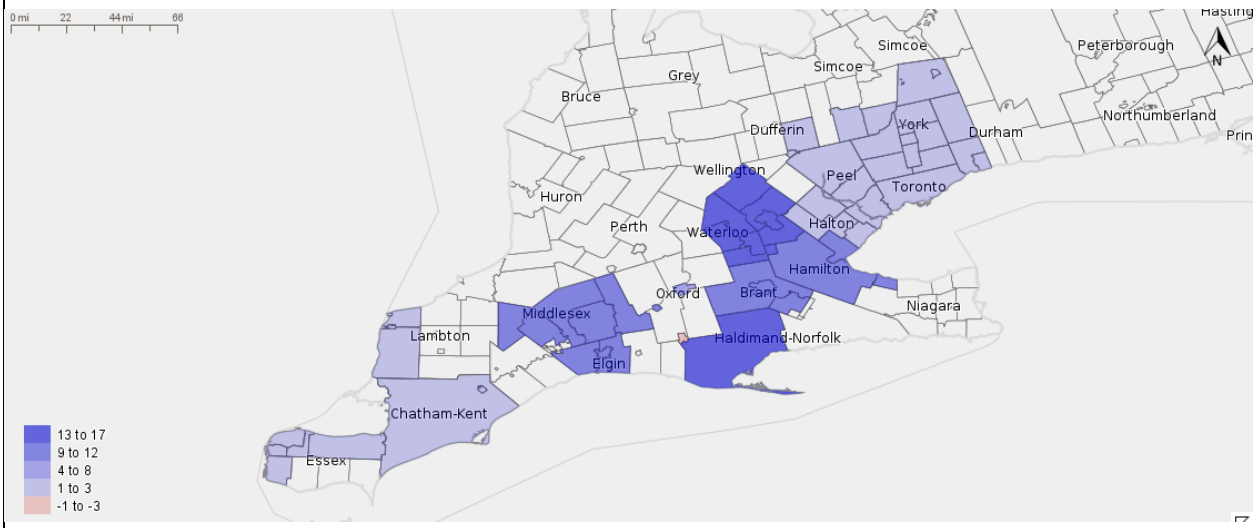
Region	2014 Jobs	2021 Jobs	Change	% Change
London CMA	1,642	1,818	176	11%
Ontario	81,289	85,678	4,389	5%
Nation	173,194	184,178	10,984	6%

Notes:

- Source: Employees and Self-Employed EMSI 2015.1

Figure and Table below show the percentage change in the number of jobs between 2014 and 2021 for CMA regions that are 100 miles from London CMA.

Figure 2. Regional percentage change in jobs (2014-2021)



Source: Employees and Self-Employed EMSI 2015.1

Table 2. CMA-level percentage change in jobs (2014-2021)

Census Metropolitan Aggregate	2014 Jobs	2021 Jobs	Change	% Change	2014 Location Quotient	2021 Location Quotient
Centre Wellington (35531)	60	71	11	18%	0.54	0.58
Norfolk (35547)	121	139	18	15%	0.52	0.57
Guelph (35550)	588	672	84	14%	0.64	0.68
Kitchener - Cambridge - Waterloo (35541)	2,429	2,771	342	14%	0.89	0.96
Hamilton (35537)	2,880	3,219	339	12%	0.85	0.89
Brantford (35543)	339	376	37	11%	0.54	0.57
London (35555)	1,642	1,818	176	11%	0.66	0.69
Ingersoll (35533)	36	40	4	11%	0.41	0.41
Woodstock (35544)	84	91	7	8%	0.35	0.35
Windsor (35559)	575	591	16	3%	0.42	0.41
Toronto (35535)	48,898	50,176	1,278	3%	1.57	1.52
Sarnia (35562)	173	177	4	2%	0.38	0.38
Chatham-Kent (35556)	165	168	3	2%	0.37	0.36
Stratford (35553)	57	57	0	0%	0.26	0.24
Tillsonburg (35546)	26	26	0	0%	0.31	0.29

Notes:

- Source: Employees and Self-Employed EMSI 2015.1

2. Job Shift Share Analysis

Job shift share analysis is a method that attempts to separate regional job growth into its components. There are three components:

1) The *national or overall effect* is the job growth attributed to the overall growth of the entire national economy.
2) The *mix or industry effect* is the job growth attributed to positive trends in the specific industry or occupation at the national level.
3) The *regional competiveness effect* is the regional growth that cannot be explained by either overall or industry occupation specific trends. This component tends to be the most important as it demonstrates a particular regional strength.

For the purposes of the analysis, *expected change* includes the national and mix effect. *Competitive effect* refers to the regional competiveness effect. *Job Change* is the difference in the number of jobs between 2021 and 2014.

For example, assume that 10 additional jobs for an occupational projection in London CMA are projected between 2014 and 2021, and 6 of these jobs are attributed to expected change and 4 to competitive change. This will imply that this occupation will increased by 6 jobs based only on the overall and industry trends. The 4 additional jobs can be attributed it to the London CMA regional trends.

Table 3. London CMA, Ontario and Canada shift share analysis (2014-2021)

	Job Change	Expected change	Competitive effect
London CMA	176	104	104
Ontario	4,388	5,156	5,156
Nation	10,985	10,985	10,985

Notes:

- Source: Employees and Self-Employed EMSI 2015.1

3. Location Quotient Analysis

Table 4 below represents the location quotient for the London CMA, Ontario and Canada for a particular occupational projection.

Location quotient is a way of quantifying how concentrated a particular occupation is in a region in comparison to the nation. For example, if the location quotient for a particular occupation in the London CMA region is 2, this occupation is 2 times more concentrated in the London CMA than the average for the whole nation.

Although not always the case, typically occupations with a high location quotient and high total job numbers are desirable since these occupations bring money into the region. It is also important to take a look at the LQ trends since high LQ with declining LQ over time would not represent something desirable for the economy.

Table 4. London CMA, Ontario and Canada location quotient analysis (2014-2021)

	2014 LQ	2021 LQ	2014-2021% Change LQ
London CMA	0.66	0.69	4.55%
Ontario	1.23	1.22	-0.81%
Nation	1.00	1.00	0.00%

Notes:

- Source: Employees and Self-Employed EMSI 2015.1

Appendix K: Support for the Program

Please find attached a letter of support for the program from Darlene O'Neill, Senior Manager of Employment and Student Entrepreneurial Services.

FANSHAWE

October 8, 2015

Tricia Tankovic
School of Information Technology

Good afternoon Tricia,

Employment and Student Entrepreneurial Services is pleased to support the Systems Operations Post-Graduate program as a Co-operative Education program. As this program will require the co-op work term to be at the end of the academic terms, it will be necessary to have students complete a work term report that is graded by an academic in order to meet the work integrated learning requirements of Co-operative Education and to ensure employers qualify for the Ontario Tax Credit.

Secondly, we support that the three year Cyber Security program currently under development be a Co-operative Education program with three work terms.

The employment rate in both of these areas is high and we are confident that the students in partnership with the Co-operative Education Consultant would be successful in achieving work terms.

Thank you for the opportunity to enage in the development of these new programs. I look forward to hearing of their successful launch.

Sincerely,

Darlene O'Neill Senior Manager

Employment and Student Entrepreneurial Services

1001 Fanshawe College Boulevard P.O. Box 7005
London ON
N5Y 5R6
fanshawec.ca

References

Government of Canada: FedDev Ontario. (2011, October 28). Government of Canada Invests in eSentire to help Safeguard Global Network Security. [Online]. Retrieved September 4th from http://www.feddevontario.gc.ca/eic/site/723.nsf/eng/00672.html.

Government of Canada: FedDev Ontario. (2012, March 23). Government of Canada Helps Accelerate Development of Innovative Security Tools. [Online]. Retrieved September 4th from http://www.feddevontario.gc.ca/eic/site/723.nsf/eng/00776.html.

Government of Canada: FedDev Ontario. (2013, September 6). Government of Canada Supports Cloud Security Innovator in Bolton. [Online]. Retrieved September 4th from http://www.feddevontario.gc.ca/eic/site/723.nsf/eng/01780.html.

Government of Canada: Public Safety Canada. (2012, October 17). Harper Government Invests in Cyber Security. [Online]. Retrieved September 4th from http://news.gc.ca/web/article-en.do?nid=701629.

Information and Communications Technology Council (ICTC). (2012). Cyber Security: Critical ICT Human Resource in the Digital Economy. [Online]. Retrieved September 4th from http://www.ictc-ctic.ca/wp-content/uploads/2012/10/ICTC_CyberSecurityReport1.pdf.